

VẤN ĐỀ ĐẠO ĐỨC VÀ AN TOÀN THÔNG TIN TRONG HỆ THỐNG THÔNG TIN

Đạo đức trong kỷ nguyên thông tin

Ethics – “Principles of right and wrong that individuals, acting as *free moral agents*, use to make choices to guide their behaviors” (Laudon, *Management Information Systems 10e*, p 128)

Computer Ethics – “Issues and standards of conduct pertaining to the use of information systems” (Jessup, *IS Today 3e*)



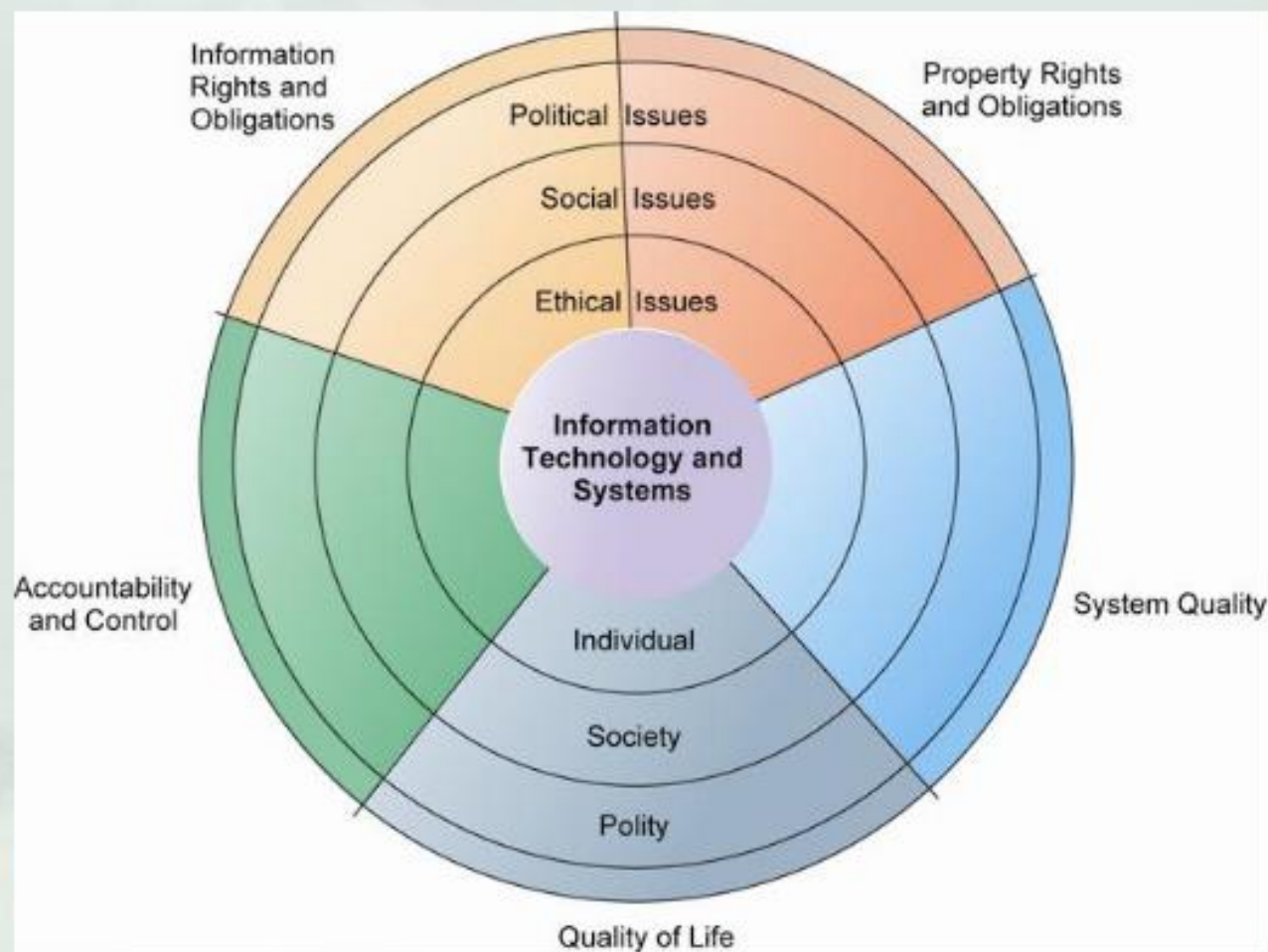
Đạo đức trong kỷ nguyên thông tin

- **Trách nhiệm (Responsibility)** – nhân tố cơ bản của hành vi đạo đức. Đó là việc chấp nhận chi phí, nhiệm vụ và nghĩa vụ đối với các quyết định của mình.
- **Trách nhiệm giải trình (Accountability)** – cơ chế để xác định các bên chịu trách nhiệm (ai có thẩm quyền thực thi nhiệm vụ và người đó phải chịu trách nhiệm trước một cá nhân hay một nhóm người nào)
- **Trách nhiệm pháp lý (Liability)** – cho phép các cá nhân (và tổ chức) khắc phục các thiệt hại do người khác gây ra cho họ
- **Quá trình/ thủ tục pháp lý (Due process)**

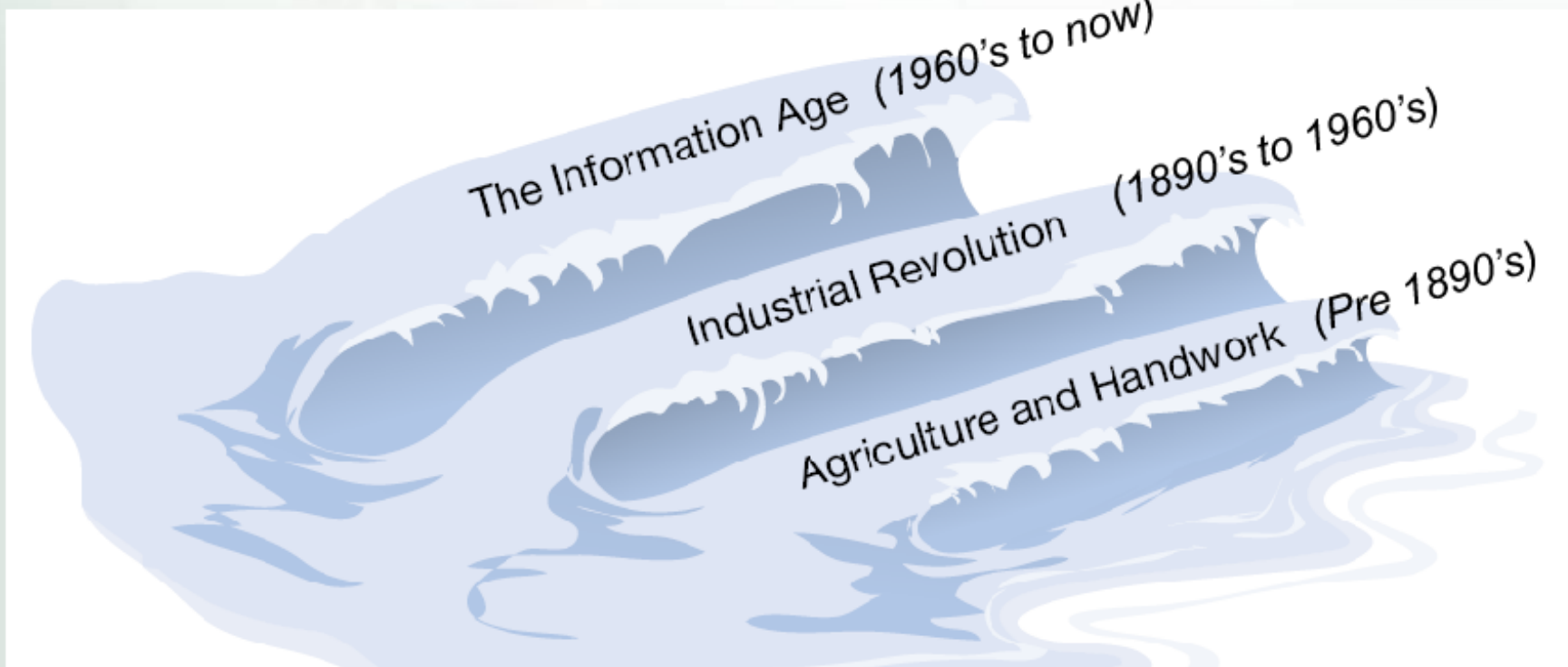
Đạo đức – Xã hội – Luật pháp trong HTTT

Đạo đức trong hệ thống thông tin

- Quyền và nghĩa vụ về thông tin
- Quyền và nghĩa vụ về tài sản thông tin
- Trách nhiệm giải trình và kiểm soát.
- Chất lượng dữ liệu và hệ thống
- Chất lượng cuộc sống



Đạo đức – Xã hội – Luật pháp trong HTTT



Các xu hướng phát triển công nghệ → vấn đề đạo đức

- Năng lực xử lý “*tăng gấp đôi*” → các tổ chức ngày càng lệ thuộc vào IS để xử lý công việc
- Giảm chi phí lưu trữ dữ liệu → khả năng lưu trữ dữ liệu cá nhân nhiều hơn và chi tiết hơn

Đạo đức – Xã hội – Luật pháp trong HTTT

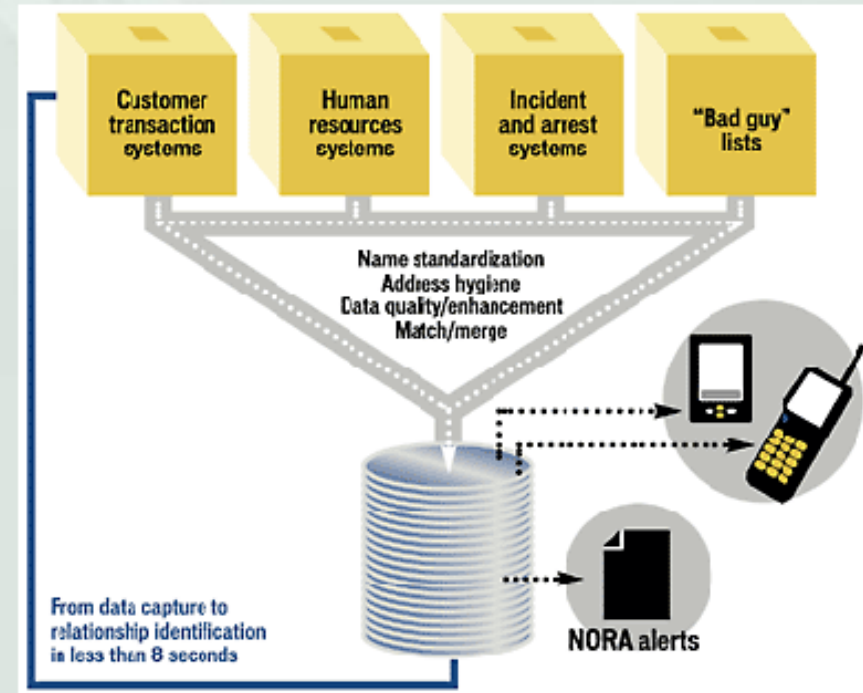
- Tiến bộ công nghệ mạng và Internet → sao chép và truy xuất thông tin từ xa dễ dàng
- Tiến bộ về kỹ thuật phân tích số liệu
 - *Profiling* – kết hợp dữ liệu từ nhiều nguồn để tạo hồ sơ về các thông tin chi tiết của cá nhân
 - *Nonobvious relationship awareness* (NORA)
- Tăng trưởng của thiết bị di động
 - Theo dõi cell phones cá nhân

Nora technology

Phần mềm NORA (*Nonobvious relationship awareness*) của SRD cho các sòng bạc ở Las Vegas để phát hiện gian lận.

Nó có thể thu thập thông tin về một cá nhân từ nhiều nguồn khác nhau và các hành vi của người đó để phát hiện các mối quan hệ mờ ám, không rõ ràng

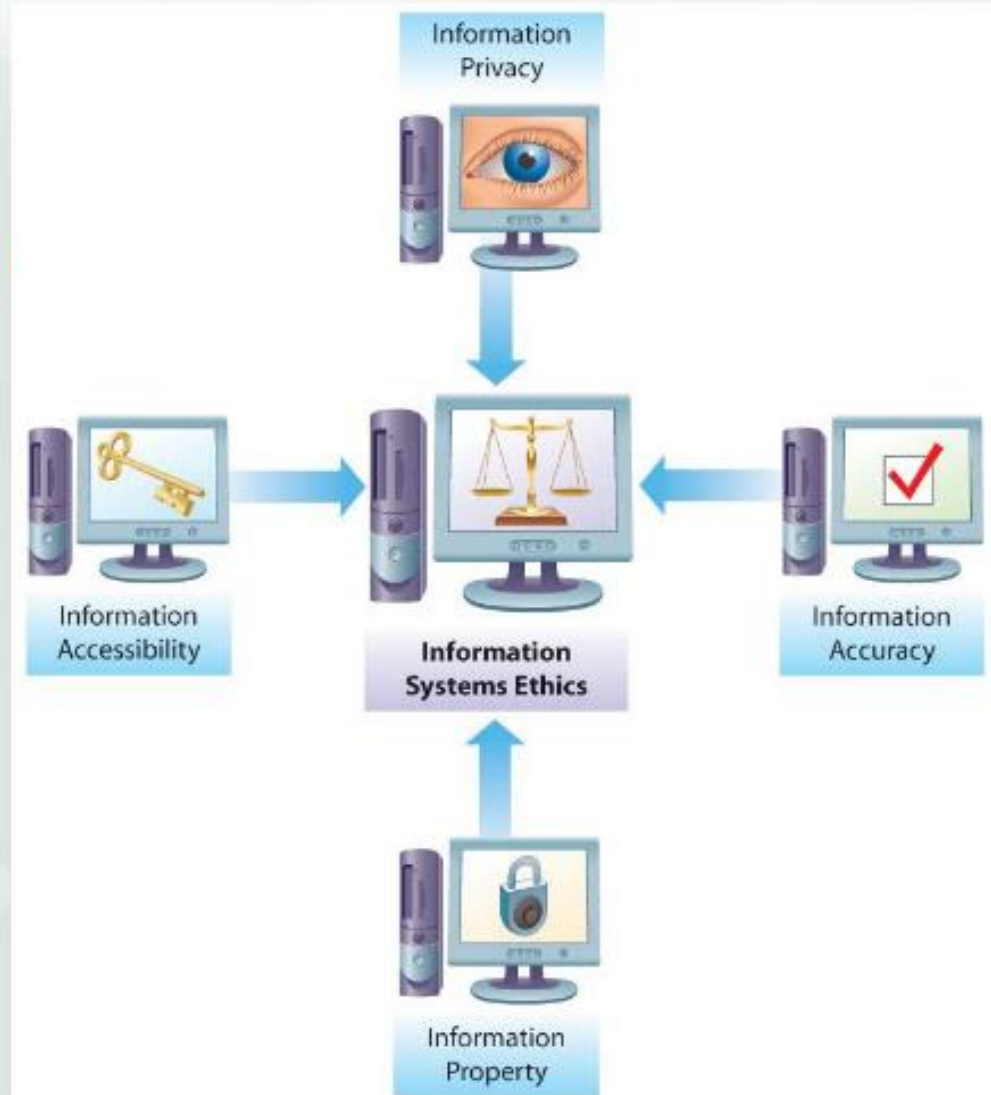
Hiện nay nó được chính phủ và khu vực tư nhân Mỹ khai thác khả năng “*Profiling*” phục vụ cho yêu cầu an ninh



Các vấn đề về chuẩn mực hành vi – Mô hình PAPA

Richard O. Mason (1986)
trong bài báo “*Four Ethical Issues of the Information Age.*” đưa ra các vấn đề liên quan đạo đức trong kỹ nguyên thông tin:

- Quyền riêng tư
- Tính chính xác
- Quyền sở hữu thông tin
- Quyền tiếp cận thông tin



Các vấn đề về chuẩn mực hành vi – Mô hình PAPA

Nguyên tắc đạo đức: Chúng ta phải bảo đảm rằng công nghệ thông tin, và các thông tin được xử lý, được sử dụng để nâng cao phẩm cách của nhân loại

Problems

Mối đe dọa

- Sự phát triển của IT, với khả năng ngày càng nâng cao của nó để giám sát, truyền thông, tính toán, lưu trữ, và phục hồi.
- Thông tin ngày càng có giá trị cao trong việc ra quyết định

Privacy

Accuracy

Property

Accessibility

Issues

- **WHAT** thông tin cá nhân hoặc hiệp hội của một cá nhân mà người đó có thể tiết lộ cho người khác; trong những điều kiện gì và những biện pháp gì để bảo vệ
- **WHAT** người ta có thể giữ riêng cho bản thân mà không bị bắt buộc phải tiết lộ cho người khác?

Quyền riêng tư – Information Privacy

Quyền riêng tư – Quyền được ở một mình, tự do không bị theo dõi hoặc can thiệp bởi các cá nhân, tổ chức, hoặc nhà nước; Quyền được kiểm soát thông tin bản thân

Các vấn đề

- “***Privacy***” vs “***Freedom of Speech***”
- Kỹ nguyên thông tin đã tác động thế nào đến “***Privacy***” ?
- Mối quan hệ hỗ tương về lợi ích giữa người thu thập thông tin cá nhân với cá nhân đó.
 - Cá nhân có thể tiết lộ hoặc giữ bí mật các thông tin?
 - Tổ chức được quyền thu thập thông tin gì; và được làm gì với các thông tin thu thập được?
 - Mô hình “***Opt-out***” vs “***Opt-in***”
- ***HOW*** bảo vệ “***Privacy***”?

Các vấn đề về chuẩn mực hành vi – Mô hình PAPA

Sự riêng tư của thông tin và vấn đề phát sinh

Tính riêng tư (Information Privacy)

Những thông tin mà cá nhân phải tiết lộ cho người khác trong quá trình xin việc hay mua hàng trực tuyến

Ăn trộm thông tin “mật”

Việc đánh cắp các thông tin riêng của cá nhân (số tài khoản, PIN ...) để mua chịu, vay tiền, mua hàng hóa, hoặc vay mượn, hay nói cách khác là những khoản nợ không bao giờ trả. Đây là vấn đề đặc biệt vì:

- Vô hình với nạn nhân, họ không biết điều gì đã xảy ra
- Rất khó sửa chữa ... bao gồm các hậu quả có thể
- Có khả năng tổn thất không thể bù đắp

Các vấn đề về chuẩn mực hành vi – Mô hình PAPA

Quản trị “tính riêng tư”

Chọn các Web sites được các tổ chức độc lập giám sát
Sử dụng các sites đánh giá để chọn các sites “an toàn” (e.g epubliceye.com)

Tránh việc lưu các Cookies trên máy
Cài đặt trình duyệt để “chặn” việc ký gửi cookies lên máy tính khi duyệt Web

Cẩn thận khi nhận các thư yêu cầu
Hãy dùng tài khoản email khác với tài khoản bình thường để bảo vệ các thông tin riêng, tránh bị xâm phạm bởi các người dùng bất kỳ trên máy tính của bạn

Quyền riêng tư – Information Privacy

Federal Trade Commission (FTC) đưa ra các nguyên tắc “Fair Information Practices (FIP)”

- ***Thông báo / nhận thức*** (nguyên tắc cốt lõi) → Website phải báo cho cá nhân biết trước khi thu thập dữ liệu.
- ***Lựa chọn / đồng ý*** (nguyên tắc cốt lõi) → Người tiêu dùng phải có khả năng lựa chọn việc thông tin của họ được sử dụng ra sao cho các mục tiêu thứ cấp.
- ***Truy cập / tham gia*** → Người tiêu dùng phải có khả năng xem xét và tranh luận về sự chính xác của dữ liệu cá nhân.
- ***An ninh*** → Người thu thập dữ liệu phải thực hiện các bước nhằm đảm bảo tính chính xác, bảo mật của dữ liệu cá nhân.
- ***Thực thi*** → Phải có cơ chế để đảm bảo việc tuân thủ các nguyên tắc FIP.

Quyền riêng tư – Internet challenge to privacy

- **Cookies** → nhận dạng trình duyệt và theo dõi việc ghé thăm trang web. → Super cookie (Flash cookies)
- **Web beacons (Web bugs)**: hình ảnh đồ họa nhỏ nhúng trong e-mail và các trang Web để giám sát người đang đọc tin nhắn e-mail hoặc truy cập vào trang web
- **Spyware**: ứng dụng “gián điệp” cài trên máy trạm nhằm lén lút thu thập thông tin cá nhân.
- **Identify Theft** → mạo danh
- Dịch vụ của Google và “**behavioral targeting**”

Các vấn đề về chuẩn mực hành vi – Mô hình PAPA

Problems	Thông tin sai lạc → quyết định sai lầm, đặc biệt khi chúng nằm trong tay những người có lợi thế về quyền lực			
	Privacy	Accuracy	Property	Accessibility
Issues	<ul style="list-style-type: none">WHO chịu trách nhiệm về khả năng xác thực, tính trung thực và chính xác của thông tin?WHO có trách nhiệm giải trình về sai sót trong thông tin và phải hành xử gì khi bị tổn thương?			

Các vấn đề về chuẩn mực hành vi – Mô hình PAPA

Tính chính xác (Information Accuracy)

Các vấn đề đảm bảo xác thực xuất xứ và tính trung thực (authenticity and fidelity) của thông tin, và xác định các trách nhiệm về các lỗi trong thông tin làm nguy hại người khác

Nguồn lỗi

Các lỗi trong kết xuất của máy tính có thể bắt nguồn từ 2 nguồn là:

- **Lỗi kỹ thuật** – lỗi giải thuật, truyền thông và/hay quá trình xử lý khi nhận, xử lý, lưu trữ, và trình bày thông tin
- **Lỗi do con người** – do người nhập dữ liệu vào hệ thống thông tin gây ra

Các vấn đề về chuẩn mực hành vi – Mô hình PAPA

Problems

- Các vấn đề đa dạng và tập trung vào lĩnh vực *tài sản trí tuệ*
→ quyền chiếm hữu, định đoạt và sử dụng

Privacy

Accuracy

Property

Accessibility

Issues

- **WHO** sở hữu thông tin?
- **WHAT** giá hợp lý và công bằng khi trao đổi thông tin?
- **WHO** sở hữu các kênh truyền, đặc biệt là kênh truyền thông?
- **HOW** được phép truy cập vào các nguồn tài nguyên khan hiếm đó?

Các vấn đề về chuẩn mực hành vi – Mô hình PAPA

Tài sản thông tin (Information property)

Tài sản thông tin liên quan đến việc ai sở hữu thông tin và thông tin có thể được bán và trao đổi như thế nào?

Ví dụ

Ai là người sở hữu thông tin được lưu trữ trong hàng ngàn cơ sở dữ liệu bởi người bán lẻ, công ty nghiên cứu tiếp thị?
→ Các công ty lưu trữ cơ sở dữ liệu về khách hàng và những người đăng ký là người sở hữu thông tin, họ được tự do buôn bán

Các vấn đề về chuẩn mực hành vi – Mô hình PAPA

Quyền sở hữu thông tin (Information Ownership)

Thuộc về các tổ chức lưu trữ thông tin nếu nó được chuyển giao ... ngay cả khi “*không nhận thức*” do sử dụng các sites đó (e.g. khảo sát trực tuyến)

Điều lệ riêng tư (Privacy Statements)

Được các tổ chức thu thập thông tin nêu ra và cách thức sử dụng chúng. Về pháp lý có 2 loại

- **Internal Use** – chỉ dùng trong phạm vi tổ chức
- **External Use** – có thể bán ra bên ngoài

Các vấn đề về chuẩn mực hành vi – Mô hình PAPA

Problems

Trình độ Tin học – Computer Literacy

- 3 Rs: **R**ead, w**R**ite, a**R**ithmetic + compute**R**

Khoảng cách số – Digital Divide

- “Knowledge is Power” Francis Bacon, 1597

Privacy

Accuracy

Property

Accessibility

Issues

- **WHAT** thông tin nào cá nhân hoặc tổ chức có quyền/ đặc ân để có được, trong các **điều kiện gì** và với các **biện pháp bảo vệ gì?**

Các vấn đề về chuẩn mực hành vi – Mô hình PAPA

Quyền truy xuất thông tin (Information Accessibility)

Các vấn đề liên quan đến việc cá nhân/ tổ chức có quyền thu thập những thông tin gì của người khác và cách thức sử dụng chúng

Ai có quyền?

- Bản thân cá nhân/ tổ chức
- Chính phủ – sử dụng các phần mềm tiên tiến (e.g. Carnivore), kiểm soát tức thời hoặc sau đó các lưu lượng email, và tất cả các hoạt động lên mạng
- Người thuê – có quyền (trong phạm vi giới hạn) giám sát, hoặc truy xuất các hoạt động trên các máy tính hay mạng của công ty khi họ đã công bố chính sách đó với nhân viên

Hành vi đạo đức

- Trong thời đại Internet, ngoài pháp chế đối với tội phạm máy tính, tính riêng tư và bảo mật còn có các chuẩn mực về đạo đức.
- Nhiều doanh nghiệp đặt ra qui tắc cho việc sử dụng công nghệ thông tin và các hệ thống máy tính một cách có đạo đức.
- Nhiều tập đoàn máy tính chuyên nghiệp cũng đặt ra những qui tắc đạo đức cho các doanh nghiệp thành viên.

Hành vi đạo đức

- Hầu hết trường đại học và nhiều hệ thống trường học cộng đồng đã đề ra những qui tắc cho sinh viên, các khoa, các phòng ban và nhân viên về đạo đức sử dụng máy tính.
- Hầu hết tổ chức và trường học động viên tất cả người dùng hệ thống hành động có trách nhiệm, đạo đức, và hợp pháp.

Hành vi đạo đức

- Những hành vi cần ngăn chặn:
 - ✓ Sử dụng máy tính để hại người khác
 - ✓ Gây cản trở công việc trên máy tính của người khác
 - ✓ Tò mò các tập tin (files) của người khác
 - ✓ Sao chép và sử dụng phần mềm không có bản quyền
 - ✓ Sử dụng tài nguyên máy tính của người khác mà chưa được cấp quyền

Hành vi đạo đức

- Những hành vi được khuyến khích:
 - ✓ Nên suy nghĩ về ảnh hưởng xã hội của những chương trình mà đang viết và các hệ thống đang thiết kế.
 - ✓ Sử dụng máy tính theo cách có cân nhắc và tôn trọng người khác.

Các hành vi phạm tội trên máy tính

1. Các hành vi truy xuất bất hợp pháp
2. Hacking và Cracking
3. Các hình thức tội phạm
4. Bản quyền phần mềm
5. Virus máy tính

Truy cập bất hợp pháp

Sử dụng máy tính để thực hiện các hành vi không hợp pháp như:

- **Thực hiện hành vi phạm tội trên máy tính** (e.g đăng nhập vào hệ thống máy tính nhằm xâm hại đến máy tính hoặc dữ liệu lưu trữ trong máy đó)
- **Dùng máy tính để phạm tội** (e.g. lấy cắp số thẻ tín dụng trong CSDL của tổ chức)
- **Sử dụng máy tính để hỗ trợ các hành vi phạm tội** (e.g. lưu thông tin về các giao dịch bất hợp pháp)

Hacking và Cracking

Hackers

Thuật ngữ dùng mô tả người truy cập trái phép vào máy tính để tìm hiểu về các máy tính đó.

- Ra đời để mô tả các sinh viên của MIT tìm cách truy cập mainframes trong những năm 1960s
- Hiện nay được dùng phổ biến để chỉ việc giành quyền truy cập trái phép với mọi lý do

Crackers

Thuật ngữ mô tả những người đột nhập hệ thống máy tính với ý đồ xâm hại hoặc thực hiện hành vi phạm tội.

- Phá hoại dữ liệu
- Đánh cắp thông tin

Các hình thức tội phạm máy tính

Có nhiều hình thức tội phạm:

- Sử dụng máy tính để đánh cắp tiền, tài sản hoặc lừa gạt tiền của người khác. Ví dụ: quảng cáo hàng giảm giá trên trang Web đấu giá, nhận đơn hàng và thanh toán sau đó gửi hàng kém chất lượng.
- Đánh cắp và thay đổi thông tin.
- Đánh cắp thông tin hoặc phá hư hệ thống máy tính sau đó tống tiền nạn nhân.

Các hình thức tội phạm máy tính

- Những tên khủng bố công nghệ (Techno-terrorists) cài đặt các chương trình phá hủy vào hệ thống máy tính sau đó đe dọa và tống tiền nạn nhân.
- Hình thức tội phạm phát tán virus làm phá hoại hệ thống máy tính hoặc ngăn chặn dịch vụ trên trang web.
- Việc sử dụng Internet làm phát sinh nhiều hình thức tội phạm như xuất hiện các trang web có nội dung không lành mạnh (phản động, đồi trụy,...)

Bản quyền phần mềm

- Những người phát triển và sản xuất phần mềm muốn bán được càng nhiều bản sản phẩm của họ càng tốt.
- Người bán không muốn bất cứ ai đó mua 1 bản phần mềm sau đó nhân ra thành nhiều bản và bán lại cho người khác.
- Nhà cung cấp cũng bị quan về khả năng các công ty mua 1 bản phần mềm ứng dụng sau đó tạo ra nhiều bản và phân phối cho nhân viên.

Virus máy tính

Viruses

Các chương trình phá hoại hoạt động bình thường của hệ thống máy tính bằng các hành vi ác ý gây nguy hại hoặc phá hủy các tập tin trên máy bị nhiễm. Các loại virus:

- **Boot Sector** – nhiễm vào phần đĩa dùng để khởi động.
- **File Infector** – nhiễm vào files như .doc, .exe, ...
- **Combination** – có khả năng hoán đổi giữa boot và file để đánh lừa các trình diệt virus
- **Attachment** – lây theo e-mail khi mở file đính kèm (attachment). Có khả năng tự gửi theo địa chỉ

Worms

Đoạn mã phá hoại có khả năng nhân bản và lan rộng trên mạng máy tính. Nó gây nguy hại bằng cách nhiễm vào bộ nhớ làm hệ thống hoạt động chậm thay vì phá hủy tập tin

Virus máy tính

Trojan Horses

Các chương trình này không có khả năng nhân bản nhưng có thể gây nguy hại bằng cách chạy ẩn các chương trình trên máy bị nhiễm (i.e một số game tự tạo account trên máy để truy cập trái phép)

Logic or Time Bombs

Biến thể Trojan Horse (không nhân bản và ẩn mình) được thiết kế để chờ sự kiện kích hoạt. (i.e. nhân viên lập trình sẽ phá hoại khi họ nghỉ việc)

- **Time Bombs** – kích hoạt bởi thời gian (e.g. sinh nhật)
- **Logic Bombs** – kích hoạt bởi tác vụ nào đó (e.g. nhập mật khẩu nào đó)

Virus máy tính

Virus phát tán theo cách:

1. Hacker tạo virus và đính kèm nó vào chương trình hoặc tập tin trên Website.
2. Người dùng tải về nghĩ rằng đó là tập tin hoặc chương trình bình thường. Khi tải xong, nó nhiễm vào các tập tin và chương trình khác trên máy tính.
3. Người dùng gửi mail, chia sẻ tập tin chứa virus cho nhiều bạn bè, đồng nghiệp.
4. Virus phát tán một cách nhanh chóng thông qua Internet.

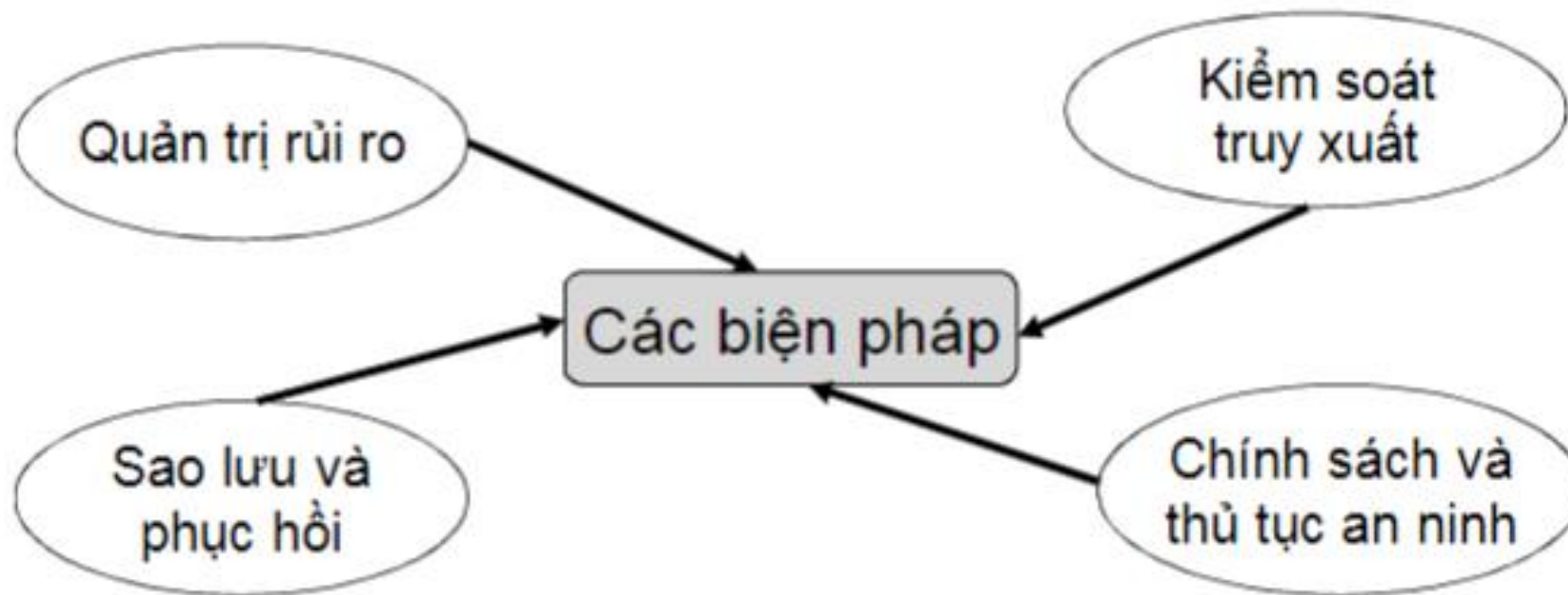
An ninh hệ thống thông tin

1. Các biện pháp quản trị an toàn
2. Các hiểm họa về an ninh và kỹ thuật phòng chống

Các biện pháp quản trị an toàn

An ninh trong hệ thống thông tin

Các biện pháp phòng ngừa giữ cho tất cả các lĩnh vực hoạt động hệ thống thông tin được an toàn khỏi các hành vi truy cập trái phép



Các biện pháp quản trị an toàn

Quản trị rủi ro

- **Kiểm toán mức độ an ninh** nhận dạng mọi lĩnh vực hệ thống thông tin và các quá trình kinh doanh
- **Phân tích rủi ro** xác định giá trị tài sản đang được bảo vệ
- **Các phương án** dựa trên phân tích rủi ro
 - **Giảm thiểu rủi ro** – hiện thực các phương án tích cực để bảo vệ hệ thống (e.g. firewalls)
 - **Chấp nhận rủi ro** – không cần biện pháp phòng chống
 - **Chuyển đổi rủi ro** – (e.g. mua bảo hiểm)

Kiểm soát truy xuất

Đảm bảo an toàn bằng cách chỉ cho phép truy xuất những gì cần để làm việc (tối thiểu)

- **Xác thực (Authentication)** – xác thực nhân thân trước khi truy xuất
- **Kiểm soát truy xuất (Access Control)**– Cấp quyền chỉ những lĩnh vực mà người dùng có quyền (e.g. accout)

Các biện pháp quản trị an toàn

Các thủ tục và chính sách

Tài liệu chính thức về cách thức sử dụng, mục tiêu và các xử lý khi không phù hợp

Sao lưu và phục hồi

- **Sao lưu** – định kỳ sao chép dự phòng các dữ liệu hệ thống thiết yếu và lưu vào nơi an toàn (e.g. backup tape)
- **Hoạch định phục hồi sự cố** – các thủ tục chi tiết được dùng để khôi phục khả năng truy xuất đến các hệ thống chủ yếu (e.g. viruses hay hỏa hoạn)
- **Phục hồi sự cố** – thực hiện các thủ tục phục hồi bằng cách dùng công cụ backup để phục hồi hệ thống về trạng thái gần nhất trước khi nó bị tổn thất

Các đe dọa an ninh và cách phòng chống

Hiểm họa an ninh

- **Mạo danh (Identity Theft)**
- **Từ chối phục vụ (Denial of Service)** – tấn công các websites qua các máy “zombie” làm tràn site → shuts down không hoạt động
- **Khác:** Spyware, Spam, Wireless Access, Viruses

Kỹ thuật phòng chống

Phổ biến gồm:

- Bức tường lửa – Firewalls
- Sinh trắc học (Biometrics)
- Mạng riêng ảo và mã hóa

Các đe dọa an ninh và cách phòng chống

a. Firewalls

Một hệ thống phần mềm, cứng hoặc cả hai được thiết kế để phát hiện các xâm nhập và ngăn chặn các truy xuất trái phép đến một hệ thống mạng riêng

Kỹ thuật được dùng

- **Lọc gói tin (Packet Filter)** – kiểm tra từng gói tin vào và ra mạng và xử lý nhận hoặc từ chối theo các luật đã xác định
- **Kiểm soát mức ứng dụng** – Thực hiện các biện pháp an ninh theo ứng dụng cụ thể (e.g. file transfer)
- **Proxy Server** – hoạt động như là máy chủ đại diện cho phép giấu địa chỉ mạng thực sự

Các đe dọa an ninh và cách phòng chống

b. Sinh trắc học – Biometrics

- Kỹ thuật nhận dạng phức tạp dùng để hạn chế truy xuất hệ thống, dữ liệu, hoặc các phương tiện
- Sử dụng các đặc tính sinh học khó làm giả để nhận dạng cá nhân như vân tay, võng mạc, ...
- Có khả năng an ninh cao

c. Mã hóa – Encryption

- Quá trình mã hóa dữ liệu trước khi truyền lên mạng và giải mã ở bên nhận
- **Public Key** – biết trước, và dùng để gửi thông điệp
- **Private Key** – không biết, và dùng để mở thông điệp
- **Certificate Authority** – tổ chức trung gian phát hành khóa