ĐẠI HỌC HUẾ
TRƯỜNG ĐẠI HỌC KINH TẾ

BÀI GIẢNG

QUẢN TRỊ RỦI RO TRONG THƯƠNG MẠI ĐIỆN TỬ

BỘ MÔN: THƯƠNG MẠI VÀ KINH DOANH QUỐC TẾ

GIẢNG VIÊN: TS. NGUYỄN THỊ DIỆU LINH
THS. DƯƠNG ĐẮC QUANG HẢO

Chương 1:
Tổng quan về rủi ro trong thương mại điện tử

GIỚI THIỆU

QUẢN TRỊ RỦI RO TRONG THƯƠNG MẠI ĐIỆN TỬ

Số tín chỉ : 02 (30 tiết)

Giảng viên : ThS Dương Đắc Quang Hảo

TS. Nguyễn Thị Diệu Linh

Điện thoại : 0905146869

Email : quanghao@hce.edu.vn

. ntdlinh@hce.edu.vn

2. Nội Quy lớp học

Tự giới thiệu về bản than

- Tên, quê quán
- Sở trường, sở đoản
- Công việc làm thêm (nếu có)
- Dự định tương lai

Tại sao quản trị rủi ro trong TMĐT lại quan trọng?

Vì sao cần quản trị rủi ro trong TMĐT

Đối với doanh nghiệp *(Báo cáo của Viện An ninh Máy tính - CSI và FBI, Mỹ)*

- Các tổ chức tiếp tục phải chịu những cuộc tấn công qua mạng từ cả bên trong lẫn bên ngoài tổ chức. Trong những tổ chức được điều tra, khoảng 90% cho rằng họ đã thấy có sự xâm phạm an ninh trong vòng 12 tháng gần nhất.

- Các hình thức tấn công qua mạng mà các tổ chức phải chịu rất khác nhau: 85% bị virus tấn công, 78% bị sử dụng trái phép mạng internet, 40% là nạn nhân của tấn công từ chối dịch vụ (DoS).

- Thiệt hại về tài chính qua các vụ tấn công qua mạng là rất lớn: 80% các tổ chức được điều tra trả lời rằng họ đã phải chịu thiệt hại về tài chính do hàng loạt các kiểu tấn công khác nhau qua mạng. Tổng thiệt hại của những tổ chức này khoảng 4,5 tỷ USD.

Đối với người tiêu dùng

- Số lượng nạn nhân của những vụ tấn công qua mạng tăng từ khoảng 127.000 vụ năm 2010 lên đến 483.000 vụ năm 2020, và con số này cao gấp 20 lần so với con số nạn nhân năm 2005.

https://vtv.vn/video/hang-gia-tran-lan-tren-mot-so-san-thuong-mai-dien-tu-490489.htm


Strategy
Rules
Policies
Process
RISK
Analysis
Control

Mục tiêu môn học

Học phần Quản trị rủi ro trong thương mại điện tử nhằm cung cấp những kiến thức cơ bản về rủi ro phát sinh trong hoạt động thương mại điện tử cũng như cách tiếp cận quản lý rủi ro trong thương mại điện tử.

Cung cấp cho sinh viên một cách có hệ thống, khoa học, đầy đủ và chi tiết những kiến thức, phương pháp và kỹ năng cần thiết về quản trị rủi ro trong thương mại điện tử:

- Tổng quan và các vấn đề rủi ro trong thương mại điện tử
- Các biện pháp phòng tránh rủi ro trong thương mại điện tử
- Thực hành quản trị rủi ro trong kinh doanh thương mại điện tử

Các nội dung chính

Chương 1: Tổng quan về rủi ro trong thương mại điện tử

1.1. Khái niệm về rủi ro trong thương mại điện tử:

1.2. Phân loại rủi ro trong thương mại điện tử

1.2.1. Rủi ro trong Thương mại điện tử có nguồn gốc khách quan

1.2.2 Rủi ro trong Thương mại điện tử có nguồn gốc chủ quan

1.3. Các khía cạnh an ninh trong thương mại điện tử

Chương 2: Nhận biết và đánh giá rủi ro trong TMĐT

2.1. Nhận biết rủi ro trong TMĐT

2.2. Phân tích rủi ro trong TMĐT

2.3. Đánh giá mối đe doạ của rủi ro trong TMĐT

Các nội dung chính

Chương 3: Kiểm soát rủi ro trong thương mại điện tử

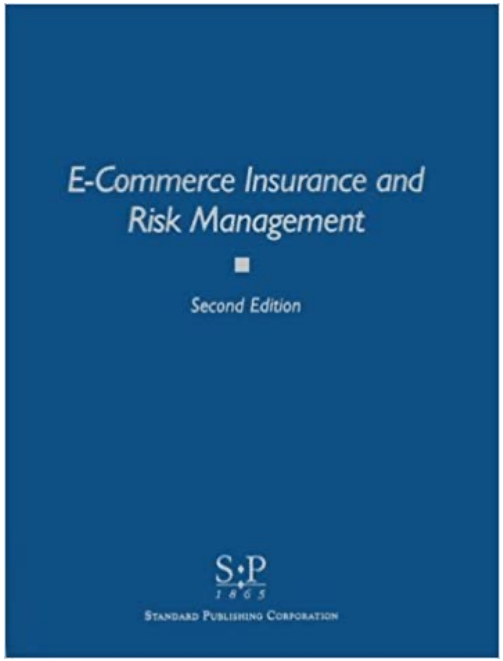
3.1. Khái niệm và chiến lược kiểm soát rủi ro trong TMĐT

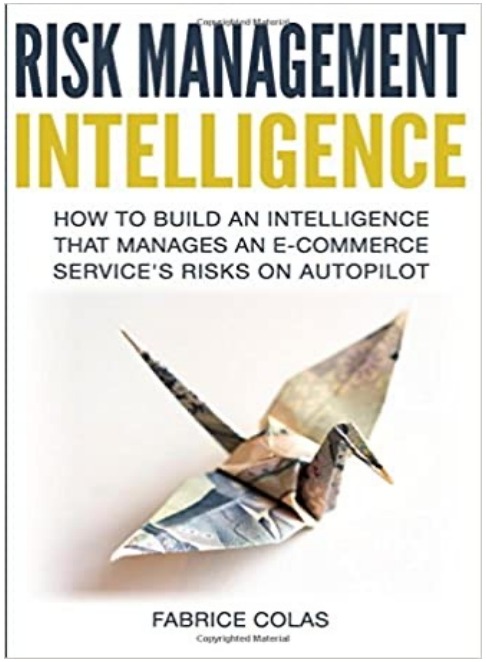
3.2. Quy trình kiểm soát rủi ro trong TMĐT

3.3. Các giải pháp kiểm soát rủi ro trong TMĐT

3.4. Biện pháp bảo vệ trong TMĐT

Tài liệu tham khảo





CHƯƠNG 1: TỔNG QUAN VỀ RỦI RO TRONG THƯƠNG MẠI ĐIỆN TỬ

ThS. Dương Đắc Quang Hào
Giảng viên
Đại học Kinh tế - Đại học Huế

Phương pháp đánh giá

Chuyên cần (10%)

- Đi học đầy đủ.
- Cho phép vắng 1 buổi.
- Vắng buổi thứ 2 trở lên: -1% / buổi.
- Trễ: -0,5% / lần.
- Không làm BTVN: -1% / lần.
- Phát biểu trên lớp, đặt câu hỏi, trả lời, trợ giảng.

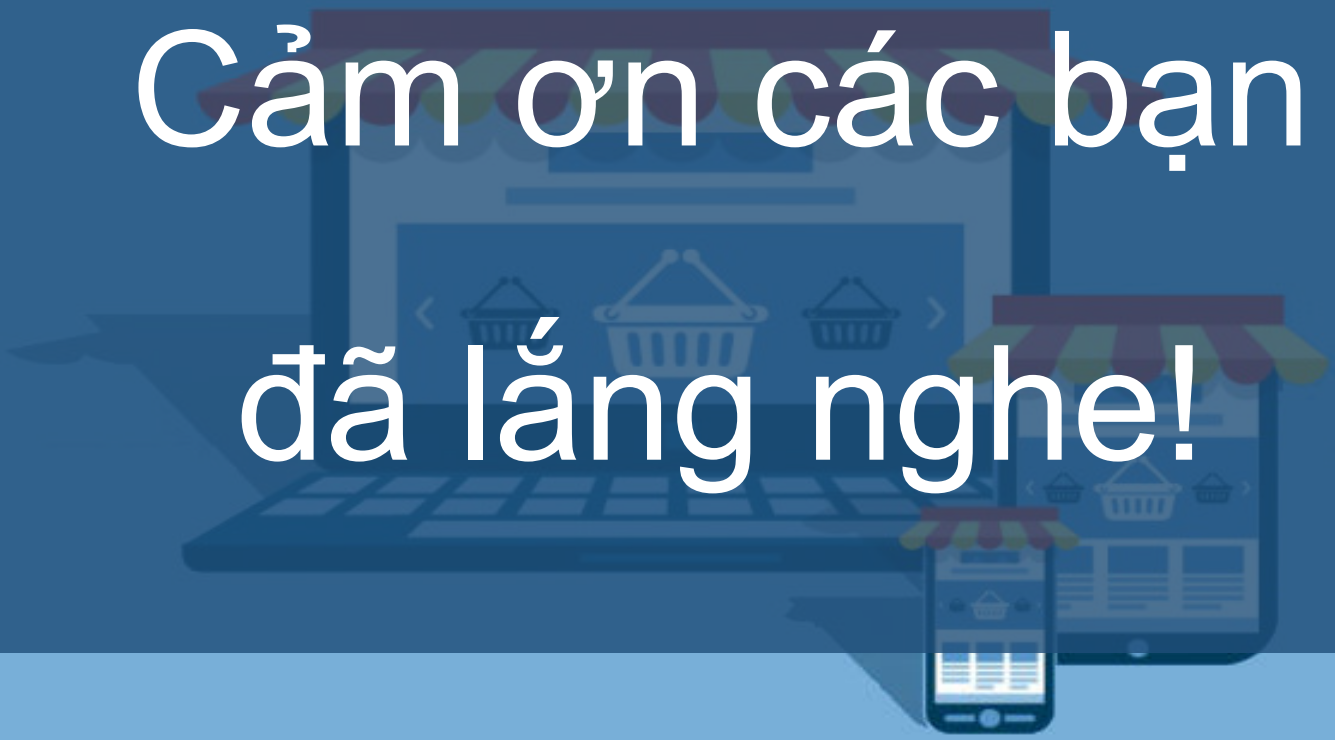
Phương pháp đánh giá

Bài tập nhóm (30%)

Lựa chọn một doanh nghiệp kinh doanh Thương mại điện tử và thực thi hoạt động quản trị rủi ro cho doanh nghiệp đó

- *Xác định các loại rủi ro doanh nghiệp đó có thể gặp phải*
- *Đo lường tác động của từng nhóm rủi ro*
- *Xây dựng các phương án phòng ngừa rủi ro cho doanh nghiệp*
- *Xây dựng các phương án để nâng cao lòng tin cho khách hàng*

Cảm ơn các bạn đã lắng nghe!



Thời gian	Trình bày	Phản biện
27/04/2022	Tuấn Anh (1)	Trọng Khiêm (2)
	Đức Phước (3)	Thanh Nhã (4)
	Nhật Huy (5)	Quốc Cường (6)

CHƯƠNG 2:
Ảnh hưởng của rủi ro tới hoạt động của doanh nghiệp trong thương mại điện tử

NỘI DUNG

1. Khái niệm về quản trị rủi ro trong TMĐT
2. Phân loại rủi ro trong thương mại điện tử
3. Các khía cạnh an ninh trong thương mại điện tử

1

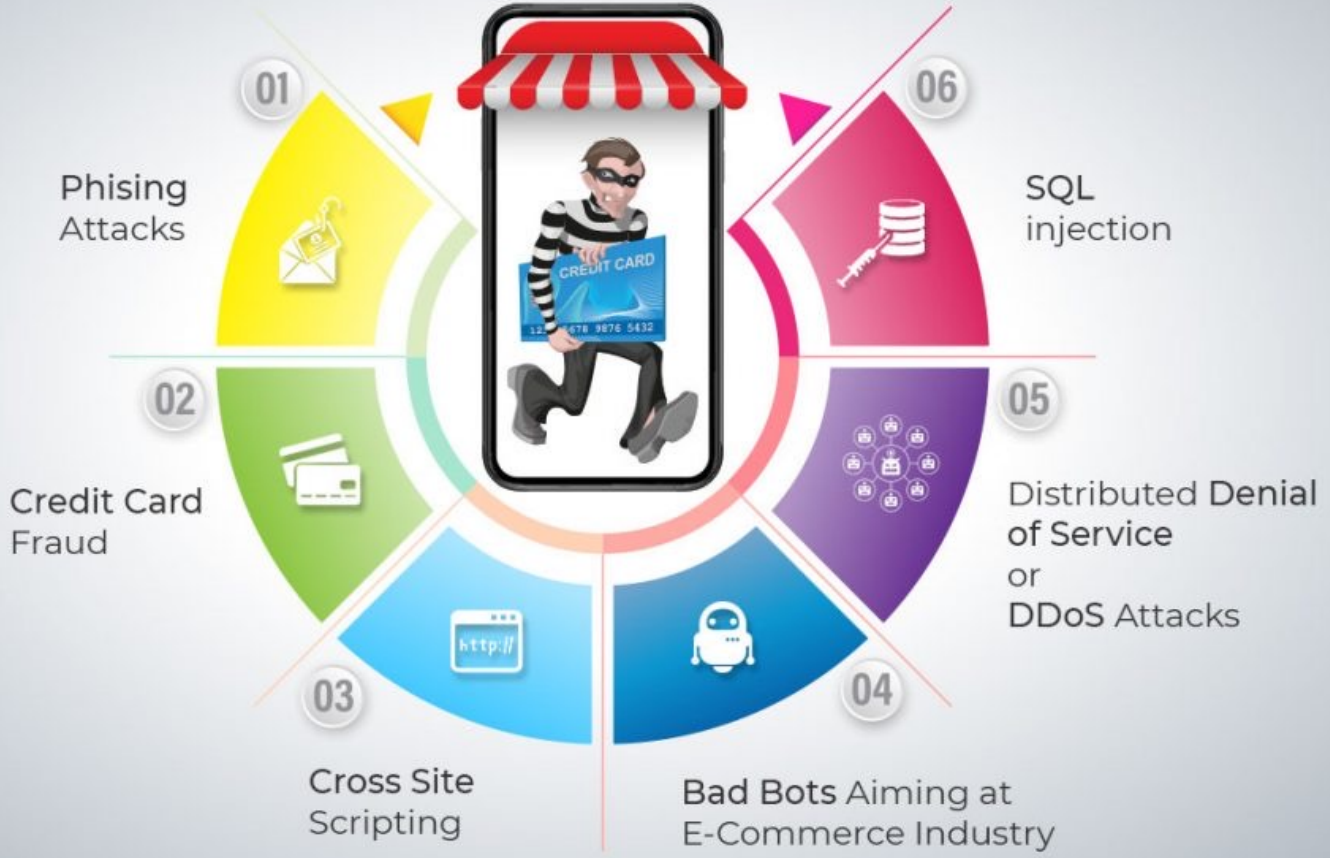
Khái niệm về quản trị rủi ro trong thương mại điện tử

RỦI RO LÀ GÌ?

Khái niệm về rủi ro trong thương mại điện tử

- Rủi ro trong kinh doanh là sự tổn thất về tài sản, các nguồn lực; sự giảm sút về lợi nhuận hay những yếu tố xảy ra ngoài ý muốn, tác động xấu đến hoạt động sản xuất kinh doanh và quá trình tồn tại, phát triển của doanh nghiệp. *(Đoàn Thị Hồng Vân)*
- Rủi ro trong TMĐT là những sự cố, xác xuất không an toàn có thể xảy ra làm thiệt hại ảnh hưởng tới việc kinh doanh, giao dịch thương mại trên internet. *(Gary Stoneburner)*

Major Threats to E-Commerce Industry



BÀI TẬP 1

Phishing attacks là gì?

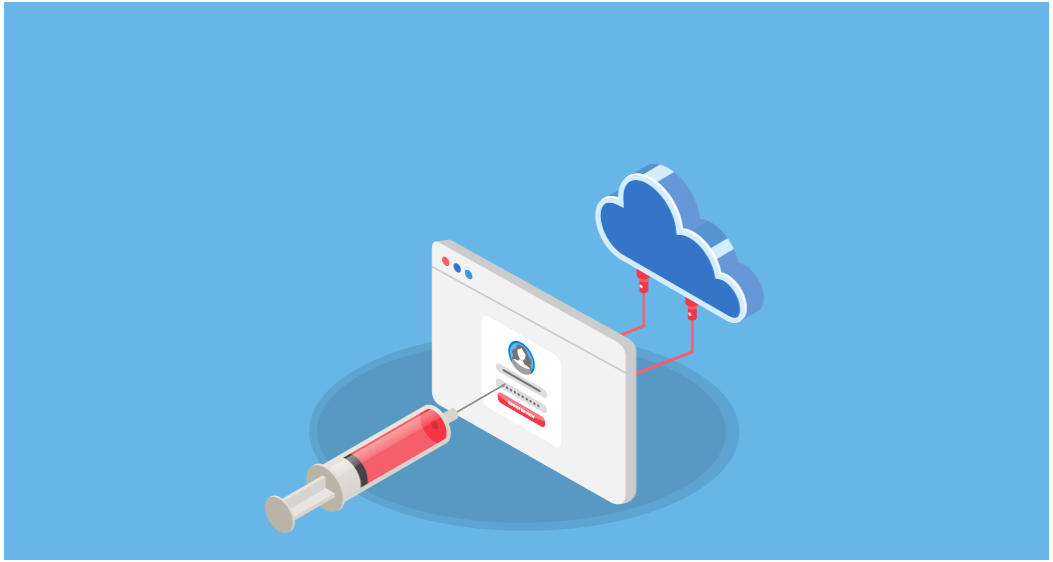
+ *Lấy ví dụ minh họa*
+ *Đối tượng thực hiện & nạn nhân*
+ *Cách thực hiện/ Cách tấn công*
+ *Cách thức xử lý khi rủi ro xảy ra*
+ *Cách thức phòng ngừa*

https://www.youtube.com/watch?v=WG8V1_Sj5g0

BÀI TẬP 2

SQL Injection là gì?

+ *Lấy ví dụ minh họa*
+ *Đối tượng thực hiện & nạn nhân*
+ *Cách thực hiện/ Cách tấn công*
+ *Cách thức xử lý khi rủi ro xảy ra*
+ *Cách thức phòng ngừa*



https://www.youtube.com/watch?v=FHCTfA9cCXs

BÀI TẬP 3

Cross Site Scripting là gì?

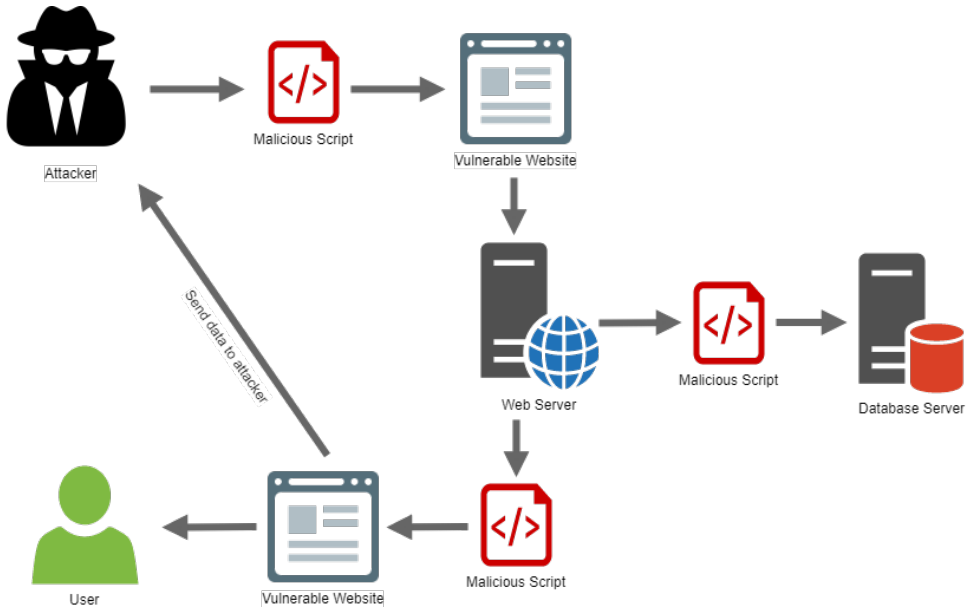
+ Lấy ví dụ minh họa

+ Đối tượng thực hiện & nạn nhân

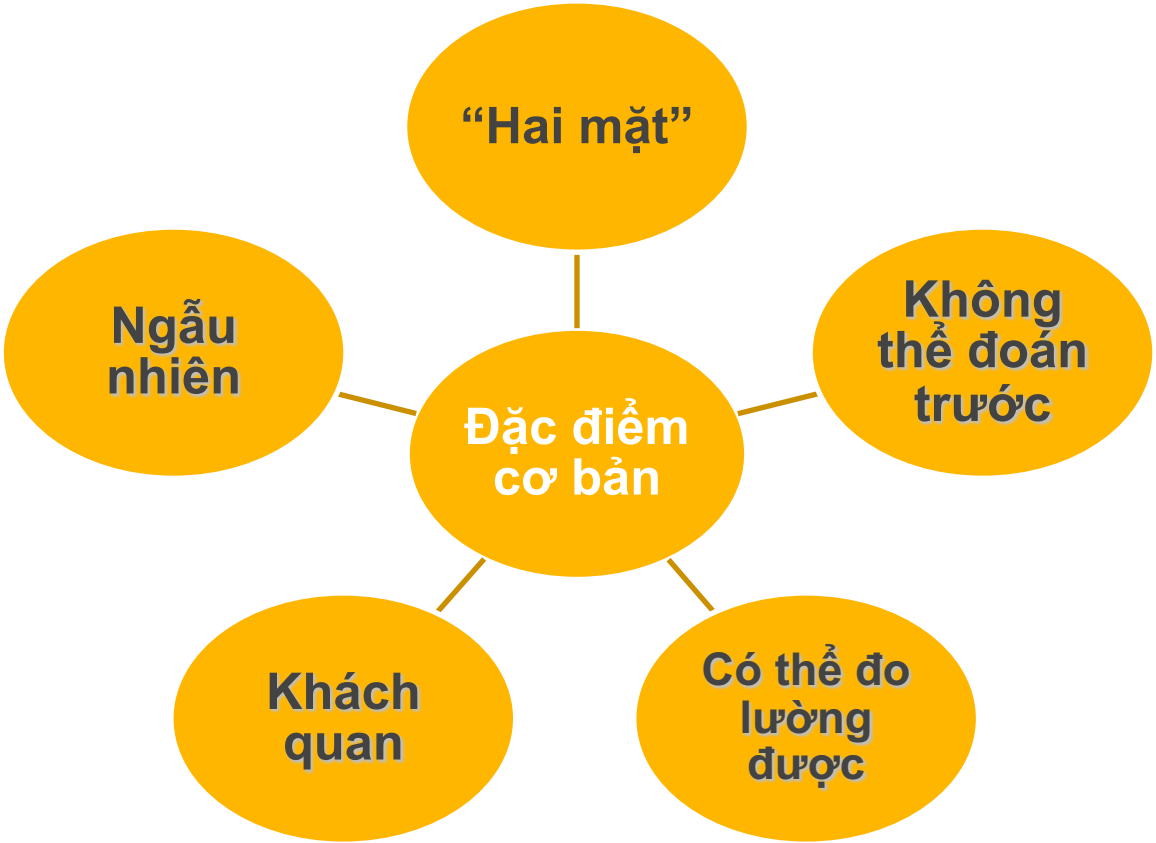
+ Cách thực hiện/ Cách tấn công

+ Cách thức xử lý khi rủi ro xảy ra

+ Cách thức phòng ngừa



https://www.youtube.com/watch?v=cbmBDiR6WaY

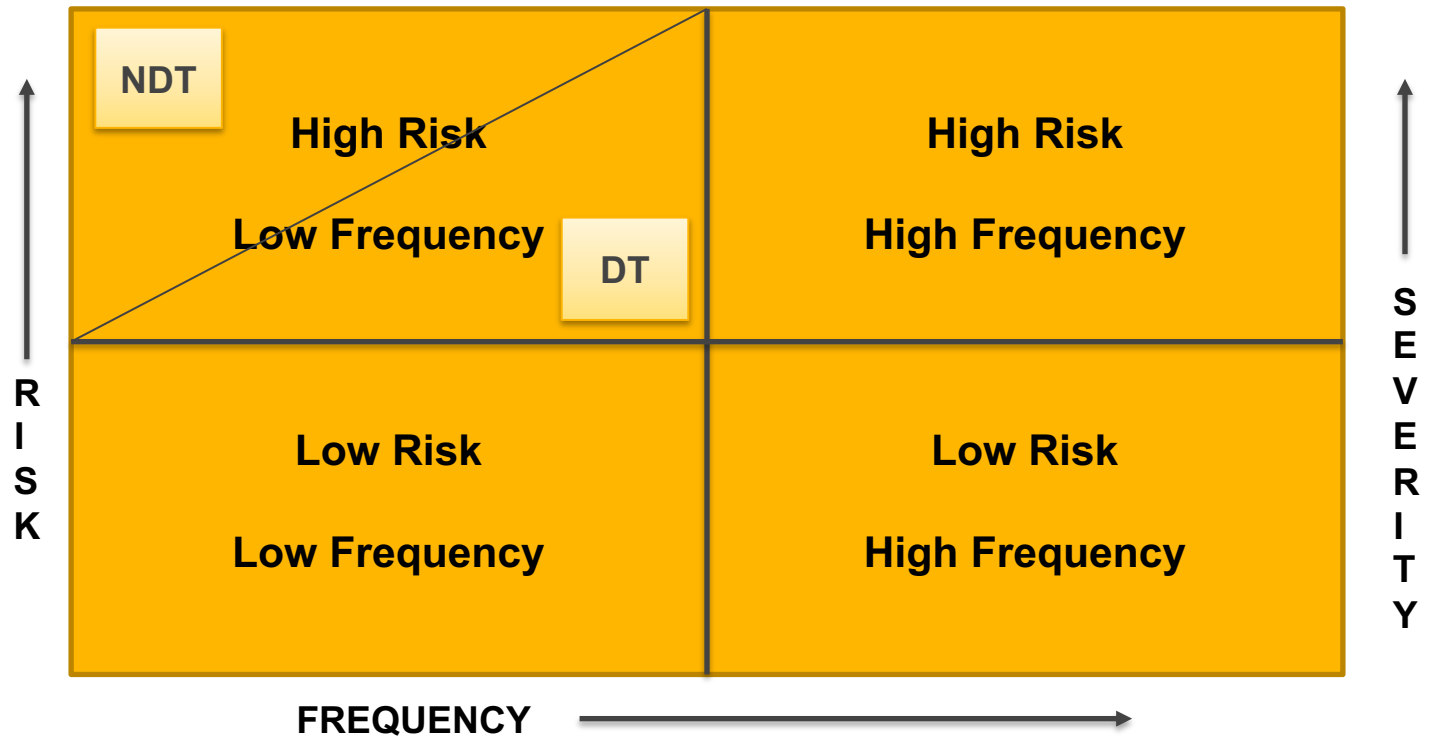

“Hai mặt”
Ngẫu nhiên
Không thể đoán trước
Đặc điểm cơ bản
Khách quan
Có thể đo lường được

Các thành phần của rủi ro

Tần suất xảy ra rủi ro (frequency/ probability)

Mức độ nghiêm trọng hay độ lớn của các rủi ro/ tổn thất có thể xảy ra (severity)

Các thành phần của rủi ro trong TMĐT



Các thành phần của rủi ro trong TMĐT

Quản trị rủi ro trong thương mại điện tử

Thái độ của con người trước rủi ro

Theo quan điểm của nhiều nhà nghiên cứu, thái độ của con người đối với rủi ro có thể chia làm 3 nhóm:

+ Nhóm 1: nhóm người thích rủi ro

+ Nhóm 2: nhóm người bàng quan với rủi ro

+ Nhóm 3: nhóm người sợ rủi ro

Quản trị rủi ro trong thương mại điện tử

Khái niệm quản trị rủi ro

Quản trị rủi ro là quá trình quản trị (**hoạch định, tổ chức, điều hành, kiểm soát**) các nguồn lực và các hoạt động nhằm làm **giảm đến mức thấp nhất** những hậu quả và những thiệt hại do rủi ro gây ra cho doanh nghiệp với **chi phí chấp nhận được.**

Quản trị rủi ro trong thương mại điện tử

Khái niệm quản trị rủi ro trong TMĐT

Quản trị RR trong TMĐT là việc bảo vệ các hệ thống và các hoạt động TMĐT từ các rủi ro có thể xảy ra cũng như việc nhận biết cơ hội, thách thức khi chúng xảy ra

Quản trị RR trong TMĐT là cách thức trong đó những tác động ngược từ rủi ro (tính 2 mặt) được quản lý và các cơ hội, tiềm năng được triển khai thực hiện. Vì vậy, quản trị RR bao hàm:

- Tối thiểu hóa các tác động, các nguồn nguy hiểm đối với hệ thống/doanh nghiệp
- Tối ưu hóa mục tiêu của doanh nghiệp.

Quản trị rủi ro trong thương mại điện tử

Nhiệm vụ của nhà quản trị rủi ro

1. **Nhận điện rủi ro**: Xây dựng quy trình, các tiêu chí nhận điện, các công cụ sử dụng và triển khai thu thập thông tin & nhận điện các rủi ro
2. **Đánh giá đo lường rủi ro**: Lựa chọn phương pháp đánh giá, công cụ sử dụng, mời chuyên gia, tổ chức đánh giá rủi ro
3. **Tham mưu xây dựng và tổ chức thực hiện chương trình kiểm soát rủi ro**:

- ✓ Thu thập và phổ biến thông tin kịp thời
- ✓ Xem xét các hợp đồng, giám sát việc soạn thảo và ký kết các hợp đồng
- ✓ Quản trị khiếu nại và kiện tụng
- ✓ Triển khai các hoạt động phòng ngừa và giảm tổn thất
- ✓ Thiết lập quan hệ với cộng đồng, chính quyền và truyền thông ….

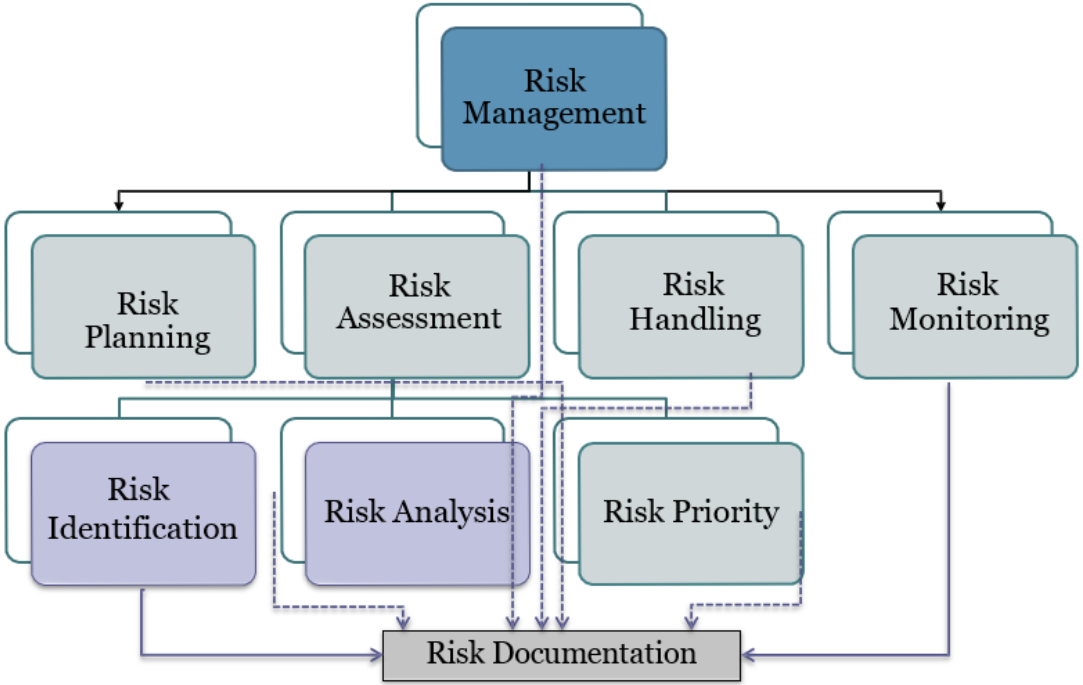
Quản trị rủi ro trong thương mại điện tử

Nhiệm vụ của nhà quản trị rủi ro

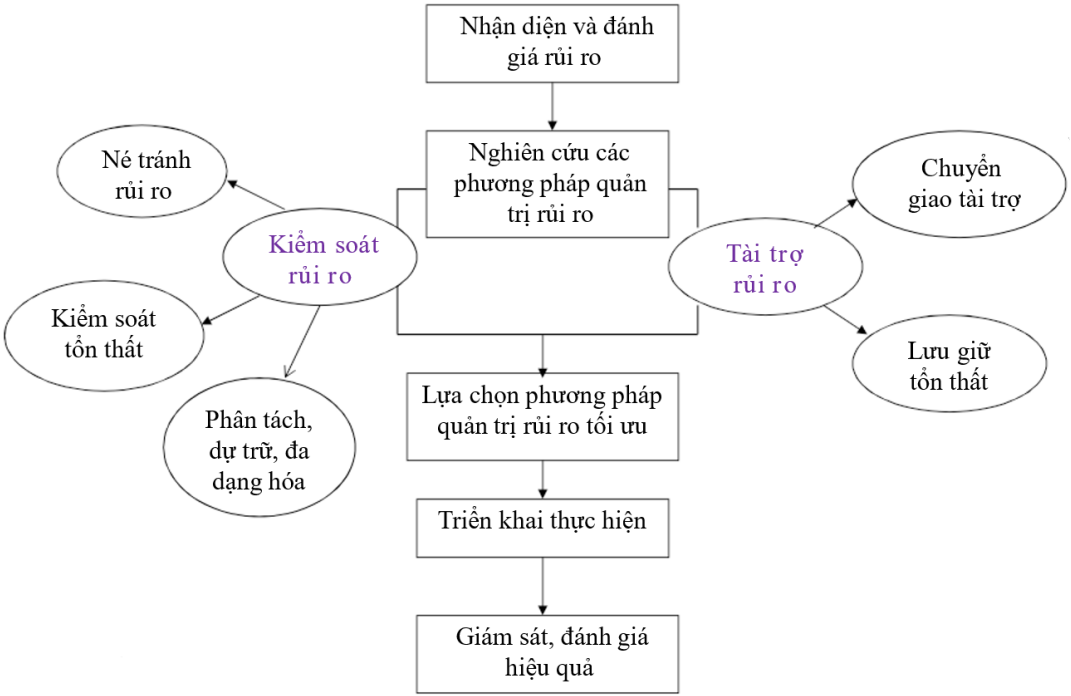
4. Tư vấn cho Ban giám đốc xây dựng và thực hiện chương trình tài trợ rủi ro

- ✓ Tư vấn, đề xuất việc mua bảo hiểm trong những trường hợp cần thiết
- ✓ Tiến hành tham gia đàm phán, ký kết các hợp đồng bảo hiểm và theo dõi quá trình thực hiện các hợp đồng này
- ✓ Sử dụng có hiệu quả Quỹ dự phòng rủi ro

Sơ đồ quy trình quản trị rủi ro



Sơ đồ quy trình quản trị rủi ro



Nguyên tắc và hạn chế quản trị rủi ro

Nguyên tắc

- Chấp nhận rủi ro (Accept No Unnecessary Risk).
- Lựa chọn rủi ro ở mức phù hợp (Make Risk Decisions at the Appropriate Level):
- Chấp nhận rủi ro khi lợi ích cao hơn chi phí (Accept Risk When Benefits Outweigh the Cost)
- Dự phòng, bảo hiểm và rủi ro

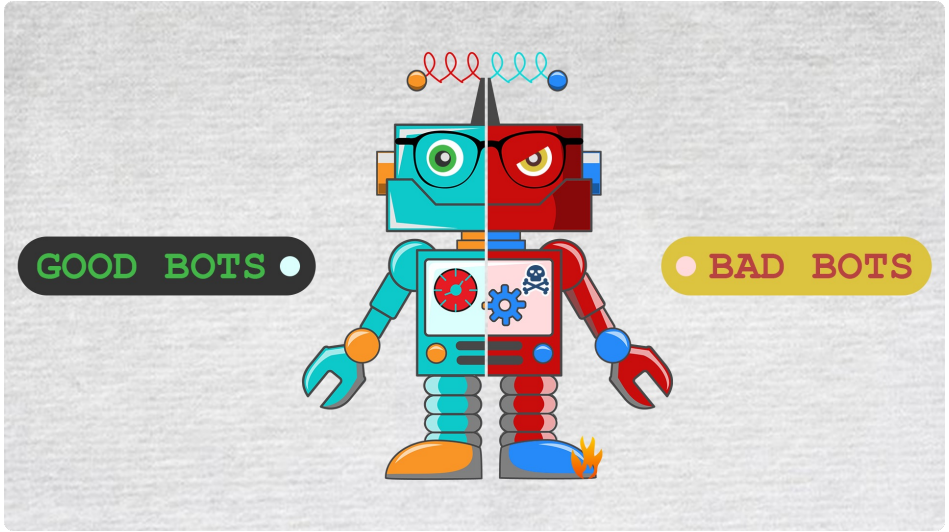
Hạn chế:

- Có thể tác động, ảnh hưởng tới các quyết định kinh doanh
- Không bảo đảm các sự cố, đe dọa sẽ không còn xảy ra
- Không loại trừ tất cả các rủi ro.

BÀI TẬP 4

Bad Bots là gì?

+ *Lấy ví dụ minh họa*
+ *Đối tượng thực hiện*
+ *Cách thực hiện*
+ *Cách thức xử lý*
+ *Cách thức phòng ngừa*



Bot? https://www.youtube.com/watch?v=UQLo399K3PE

What is Bot? https://www.youtube.com/watch?v=fEbzk4vTHsQ

BÀI TẬP 5

Credit Card Fraud là gì?

+ Lấy ví dụ minh họa

+ Đối tượng thực hiện

+ Cách thực hiện

+ Cách thức xử lý

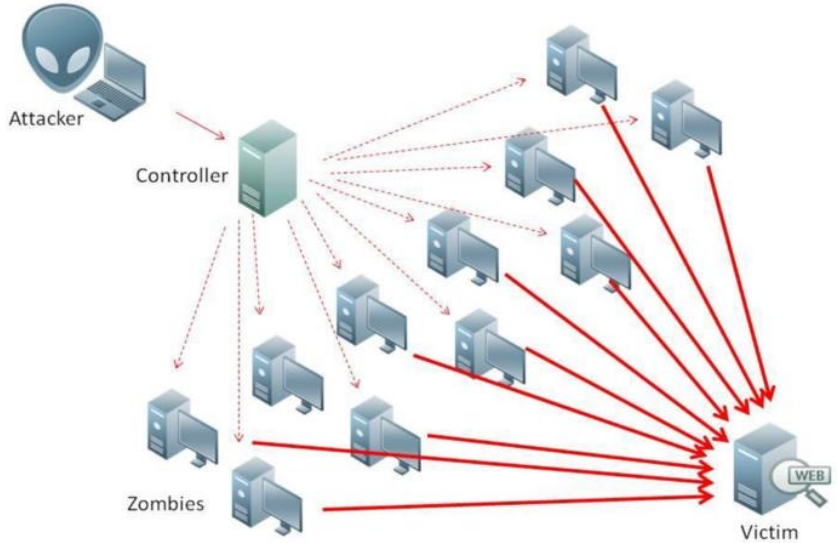
+ Cách thức phòng ngừa

https://www.youtube.com/watch?v=AWAfyjts4xk

BÀI TẬP 6

DDoS attacks (Distributed Denial of service) là gì?

+ *Lấy ví dụ minh họa*
+ *Đối tượng thực hiện*
+ *Cách thực hiện*
+ *Cách thức xử lý*
+ *Cách thức phòng ngừa*



https://www.youtube.com/watch?v=yLbC7G71lyE

2

Phân loại rủi ro trong thương mại điện tử

Phân loại rủi ro trong thương mại điện tử

Theo nguồn phát sinh rủi ro	Theo tiến trình kinh doanh TMĐT	Theo đối tượng chịu tác động
Rủi ro khách quan Rủi ro chủ quan	Rủi ro thị trường Rủi ro từ khách hàng Rủi ro từ nhà cung ứng Rủi ro trong vận chuyển Rủi ro trong giao nhận hàng Rủi ro trong thanh toán	Rủi ro về dữ liệu Rủi ro về công nghệ Rủi ro về các thủ tục quy trình giao dịch Rủi ro về luật pháp và quy trình công nghệ

❶ Phân loại rủi ro theo nguồn phát sinh

Rủi ro trong thương mại điện tử có nguồn gốc **khách quan**

- Rủi ro do thiên tai
- Rủi ro do các tai nạn bất ngờ
- Rủi ro do các hiện tượng xã hội gây nên
- Rủi ro do những hành động cố ý của các cá nhân

❶ Phân loại rủi ro theo nguồn phát sinh

Rủi ro trong thương mại điện tử có nguồn gốc **chủ quan**

- Rủi ro do lừa đảo
- Rủi ro do nghẽn mạng giao dịch
- Rủi ro do vi phạm quyền sở hữu trí tuệ
- Rủi ro an toàn bảo mật
- Rủi ro do sự bất cẩn của người sử dụng
- Rủi ro khước từ phục vụ (DoS-denial of service)
- Kẻ trộm trên mạng (sniffer)
- Rủi ro trong việc sử dụng và quản lý mạng
- Rủi ro gian lận thẻ tín dụng

Từ con người

- Hackers
- Ex-employees
- Intruders

Từ môi trường (Environmental)

- Hỏa hoạn (Fires)
- Vi rút (Viruses)
- Power Outages

Tự nhiên Natural

- Lũ lụt (Floods)
- Động đất (Earthquakes)
- Sóng thần (Tornadoes)

Phân loại rủi ro trong thương mại điện tử

Theo nguồn phát sinh rủi ro	Theo tiến trình kinh doanh TMĐT	Theo đối tượng chịu tác động
Rủi ro khách quan Rủi ro chủ quan	Rủi ro thị trường Rủi ro từ khách hàng Rủi ro từ nhà cung ứng Rủi ro trong vận chuyển Rủi ro trong giao nhận hàng Rủi ro trong thanh toán	Rủi ro về dữ liệu Rủi ro về công nghệ Rủi ro về các thủ tục quy trình giao dịch Rủi ro về luật pháp và quy trình công nghệ

❷ Phân loại rủi ro theo đối tượng chịu tác động

2.1. Rủi ro về dữ liệu

Rủi ro về dữ liệu đối với người bán

- Thay đổi địa chỉ nhận đối với chuyển khoản ngân hàng và do vậy chuyển khoản này sẽ được chuyển tới một tài khoản khác của người xâm nhập bất chính.
- Nhận được những đơn đặt hàng giả mạo. Trong trường hợp một khách hàng quốc tế đặt hàng và sau đó từ chối hành động này, người bán hàng trực tuyến thường không có cách nào để xác định rằng thực chất hàng hóa đã được giao đến tay khách hàng hay chưa và chủ thẻ tín dụng có thực sự là người đã thực hiện đơn đặt hàng hay không.

❷ Phân loại rủi ro theo đối tượng chịu tác động

2.1. Rủi ro về dữ liệu

Rủi ro về dữ liệu đối với người mua

- Thông tin bí mật về tài khoản bị dánh cắp khi tham gia giao dịch thương mại điện tử.
- Hiện tượng các trang web giả mạo, giả mạo địa chỉ Internet (IP Spoofing), phong tỏa dịch vụ (DOS – denial of service), và thư điện tử giả mạo của các tổ chức tài chính ngân hang.
- Tin tặc tấn công và các website thuong mại điện tử, truy cập các thông tin về thẻ tín dụng.

❷ Phân loại rủi ro theo đối tượng chịu tác động

2.1. Rủi ro về dữ liệu

Rủi ro về dữ liệu đối với chính phủ

- Các hacker có nhiều kỹ thuật tấn công các trang web này nhằm làm lệch lạc thông tin, dánh mất dữ liệu thậm chí là đánh “sập” khiến các trang web này ngừng hoạt động.
- Đặc biệt một số tổ chức tội phạm đã sử dụng các tin tặc để phát động các cuộc tấn công mang tính chất chính trị hoặc tương tự nhu vậy.

❷ Phân loại rủi ro theo đối tượng chịu tác động

2.2. Rủi ro liên quan đến công nghệ

Xét trên góc độ công nghệ thì có 3 bộ phận dễ bị tấn công và tổn thương nhất khi thực hiện giao dịch thương mại điện tử:

- Hệ thống của khách hàng: có thể là doanh nghiệp hay cá nhân
- Máy chủ của doanh nghiệp: ISP – nhà cung cấp dịch vụ (Internet service provider), Người bán, Ngân hàng.
- Đường dẫn thông tin (communication pipelines)

❷ Phân loại rủi ro theo đối tượng chịu tác động

2.2. Rủi ro liên quan đến công nghệ

Rủi ro về gian lận thẻ tín dụng

Trong thương mại điện tử, các hành vi gian lận thẻ tín dụng xảy ra đa dạng và phức tạp hơn nhiều so với thương mại truyền thống.Trong thương mại điện tử mối đe doạ lớn nhất là bị “mất”(hay bị lộ) các thông tin liên quan đến thẻ tín dụng hoặc các thông tin giao dịch sử dụng thẻ tín dụng trong quá trình diễn ra giao dịch.

❷ Phân loại rủi ro theo đối tượng chịu tác động

2.2. Rủi ro liên quan đến công nghệ

Kẻ trộm trên mạng (sniffer)

- Kẻ trộm trên mạng (sniffer) là một dạng của chương trình nghe trộm, giám sát sự di chuyển của thông tin trên mạng. Khi sử dụng vào những mục dích hợp pháp, nó có thể giúp phát hiện ra những yếu diểm của mạng, nhưng ngược lại, nếu sử dụng vào các mục đích phạm tội, nó sẽ trở thành các mối nguy hiểm khó lường và rất khó có thể phát hiện.
- Xem lén thư điện tử là một dạng mới của hành vi trộm cắp trên mạng. Kỹ thuật xem lén thư điện tử sử dụng một doạn mã ẩn bí mật gắn vào thông điệp thu điện tử, cho phép người nào đó có thể giám sát toàn bộ các thông điệp chuyển tiếp dược gửi đi cùng với thông điệp ban đầu.

❷ Phân loại rủi ro theo đối tượng chịu tác động

2.3. Rủi ro liên quan đến thủ tục, quy trình giao dịch của tổ chức

- Nhiều website vẫn tiến hành bán hàng theo các yêu cầu mà không có bất kỳ sự xác thực cần thiết và cẩn trọng nào về thông tin của người mua. Họ đưa ra các đơn chào hàng và tiến hành giao hàng nếu nhận đươc chấp nhận chào hàng từ phía người mua.
- Do không có những biện pháp đảm bảo chống phủ định của người mua trong quy trình giao dịch trên các website nên không thể buộc người mua phải nhận hàng hay thanh toán khi đơn đặt hàng đã được thực hiện và hàng đã giao.

❷ Phân loại rủi ro theo đối tượng chịu tác động

2.3. Rủi ro liên quan đến thủ tục, quy trình giao dịch của tổ chức

- Hay những đơn đặt hàng không được nhà cung cấp thực hiện trong khi khách hàng đã tiến hành trả tiền mà không nhận được hàng, nhà cung cấp từ chối đã nhận đơn đặt hàng.
- Khi các bên thảo luận một hợp đồng thương mại qua hệ thống điện tử, hợp đồng đó sẽ có thể được thiết lập bằng cách một bên đưa ra lời chào hàng và bên kia chấp nhận lời chào hàng. Sự tồn tại của một hợp đồng có thể gây tranh cãi nếu bạn không có bằng chứng về sự hình thành hợp đồng. Doanh nghiệp sử dụng một phương tiện điện tử (như e-mail) trong quá trình thiết lập một hợp đồng thì rủi ro do không lường trước được.

❷ Phân loại rủi ro theo đối tượng chịu tác động

2.4. Rủi ro liên quan đến pháp luật và tiêu chuẩn công nghiệp

Hiệu lực pháp lý của giao dịch thương mại điện tử.

- Nước ta mặc dù đã có luật về giao dịch điện tử, trong đó thừa nhận giá trị pháp lý của các tài liệu điện tử.
- Tuy nhiên làm thế nào để đảm bảo rằng một thoả thuận đạt được qua hệ thống điện tử sẽ có tính ràng buộc về mặt pháp lý khi có sự khác nhau giữa các hệ thống pháp luật khác nhau.

Ví dụ: Việt Nam và Nhật Bản? Chưa có một công ước chung nào về giao dịch thương mại điện tử có hiệu lực sẽ gây trở ngại trong việc giải quyết tranh chấp khi hợp đồng bị vi phạm. Lấy đơn giản là ASEAN, chưa có quy định nội khối chính thức điều chỉnh giao dịch điện tử.

❷ Phân loại rủi ro theo đối tượng chịu tác động

2.4. Rủi ro liên quan đến pháp luật và tiêu chuẩn công nghiệp

- Các quy định cản trở sự phát triển của TMĐT hoặc chưa tạo điều kiện thuận lợi cho phát triển TMĐT như đăng ký website, mua bán tên miền; sự chậm trễ về dịch vụ chứng thực điện tử, thanh toán điện tử một phần là do thiếu các văn bản pháp lý diều chỉnh Rủi ro về tiêu chuẩn công nghiệp.

- Thiếu một hạ tầng công nghệ thông tin đồng bộ và chưa có một hệ thống các tiêu chuẩn công nghiệp phù hợp với tiêu chuẩn quốc tế và khu vực. Sự thiếu đồng bộ về tiêu chuẩn công nghiệp sẽ gây nhiều khó khăn trong việc trao đổi thông tin và đặc biệt là hoạt động chào hàng, đặt hàng cũng như vận chuyển hàng hoá, thủ tục hải quan, thuế…

- Mặt khác sự khác biệt giữa tiêu chuẩn công nghiệp trong thương mại truyền thống và thương mại điện tử cũng có thể gây ra những rủi ro không mong dợi. Đặc biệt đối với những hàng hoá vô hình như các loại dịch vụ trên Internet thì hiện nay vẫn chưa có một hệ thống tiêu chuẩn công nghiệp nào để đánh giá chính xác.

Phân loại rủi ro trong thương mại điện tử

Theo nguồn phát sinh rủi ro	Theo tiến trình kinh doanh TMĐT	Theo đối tượng chịu tác động
Rủi ro khách quan Rủi ro chủ quan	Rủi ro thị trường Rủi ro từ khách hàng Rủi ro từ nhà cung ứng Rủi ro trong vận chuyển Rủi ro trong giao nhận hàng Rủi ro trong thanh toán	Rủi ro về dữ liệu Rủi ro về công nghệ Rủi ro về các thủ tục quy trình giao dịch Rủi ro về luật pháp và quy trình công nghệ

❸ Phân loại rủi ro theo tiến trình kinh doanh TMĐT

3.1. Rủi ro thị trường (market risk)

- Khó xác định tổng cầu trực tuyến, khả năng bị động trong dự trữ hàng hóa.
- Khủng hoảng thừa ➔ nguy cơ giảm giá, tăng chi phí, tồn kho quá mức;
- Khủng hoảng thiếu ➔ không đáp ứng nhu cầu đặt hàng kịp thời, đúng lúc
- Mua hàng có tính mùa vụ
- Tập khách hàng không ổn định, sự di chuyển quá nhanh của khách hàng trên web, nhiều sự lựa chọn, giữ khách hàng ở lại web khó khăn
- Nhu cầu, thị hiếu khách hàng thay đổi quá nhanh
- Hàng tăng giá khi đã chấp nhận đơn hàng trực tuyến

❸ Phân loại rủi ro theo tiến trình kinh doanh TMĐT

3.2. Rủi ro khách hàng

- Những khách hàng lần đầu giao dịch
- Khách hàng mua hàng với số lượng lớn
- Khách hàng đến từ thị trường đã có cảnh báo
- Khách hàng sử dụng địa chỉ email miễn phí để đặt hàng
- Đơn đặt hàng yêu cầu gửi hàng nhanh và khẩn cấp
- Đơn đặt hàng yêu cầu gửi hàng đến các quốc gia, khu vực có cảnh báo rủi ro cao

❸ Phân loại rủi ro theo tiến trình kinh doanh TMĐT

3.2. Rủi ro khách hàng

- Nhiều thẻ thanh toán một đơn hàng và yêu cầu gửi hàng đến một địa chỉ
- Một thẻ thực hiện nhiều giao dịch trong một thời gian ngắn
- Một thẻ thực hiện nhiều giao dịch và yêu cầu gửi hàng đến nhiều địa chỉ khác nhau
- Nhiều thẻ được thanh toán từ một địa chỉ Internet (IP)
- Khó xây dựng khách hàng trung thành so với bán hàng truyền thống

❸ Phân loại rủi ro theo tiến trình kinh doanh TMĐT

3.3. Rủi ro vận chuyển hàng hóa (shipping & delivery risk)

- Container hàng từ nhà cung ứng nước ngoài bị ách tắc ở Hải Quan bởi sự thay đổi chính sách hoặc sự cố trong quá trình vận chuyển, dẫn tới không có hàng để bán.

❸ Phân loại rủi ro theo tiến trình kinh doanh TMĐT

3.3. Rủi ro trong giao hàng

- Hàng hóa vật thể: đối với thanh toán COD, khách hàng có thể không nhận hàng (ko nghe điện thoại, tránh né, đưa ra các lí do khác…) ➔ gây khó khăn cho nhân viên giao hàng, làm tăng chi phí vận chuyển
- Hàng hóa không phù hợp với đơn hàng
- Hàng số hóa: vấn đề bản quyền và các RR thông tin (CIA). Giao hàng số hóa liên quan đến truyền thông tin, dữ liệu qua mạng Internet và mạng truyền thông có thể bị chặn giữ, chỉnh sửa…

❸ Phân loại rủi ro theo tiến trình kinh doanh TMĐT

3.4. Rủi ro trong thanh toán

- Gian lận trong thanh toán điện tử
- Sơ xuất, lỗi trong chuyển khoản
- DN bị hạn chế trong công tác xác thực khách hàng: không kiểm tra được thẻ vật lý, hóa đơn không có chữ ký của người mua.
- Giao dịch thanh toán thành công trên cổng thanh toán trực tuyến chưa phải là một giao dịch mua bán hàng hóa thành công.

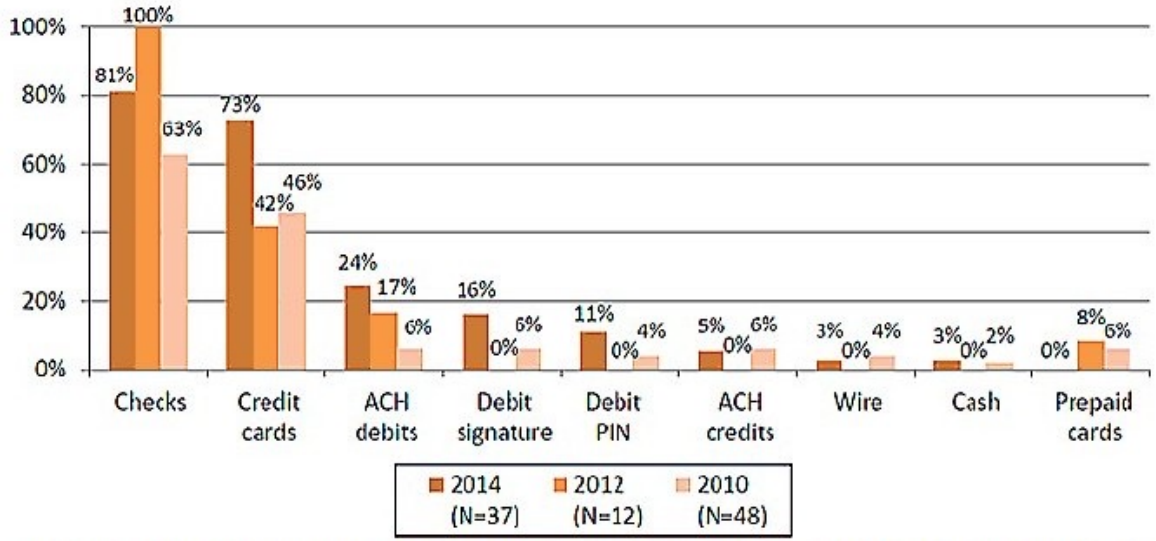
❸ Phân loại rủi ro theo tiến trình kinh doanh TMĐT

3.4. Rủi ro trong thanh toán

- Người bán không phát hiện được hiệu lực của thẻ đã hết hạn
- Người bán hàng vượt hạn mức cho phép mà không nhận được sự đồng ý của đơn vị cấp phép
- Sửa chữa số tiền trên hóa đơn
- Người mua thay đổi quyết định mua,

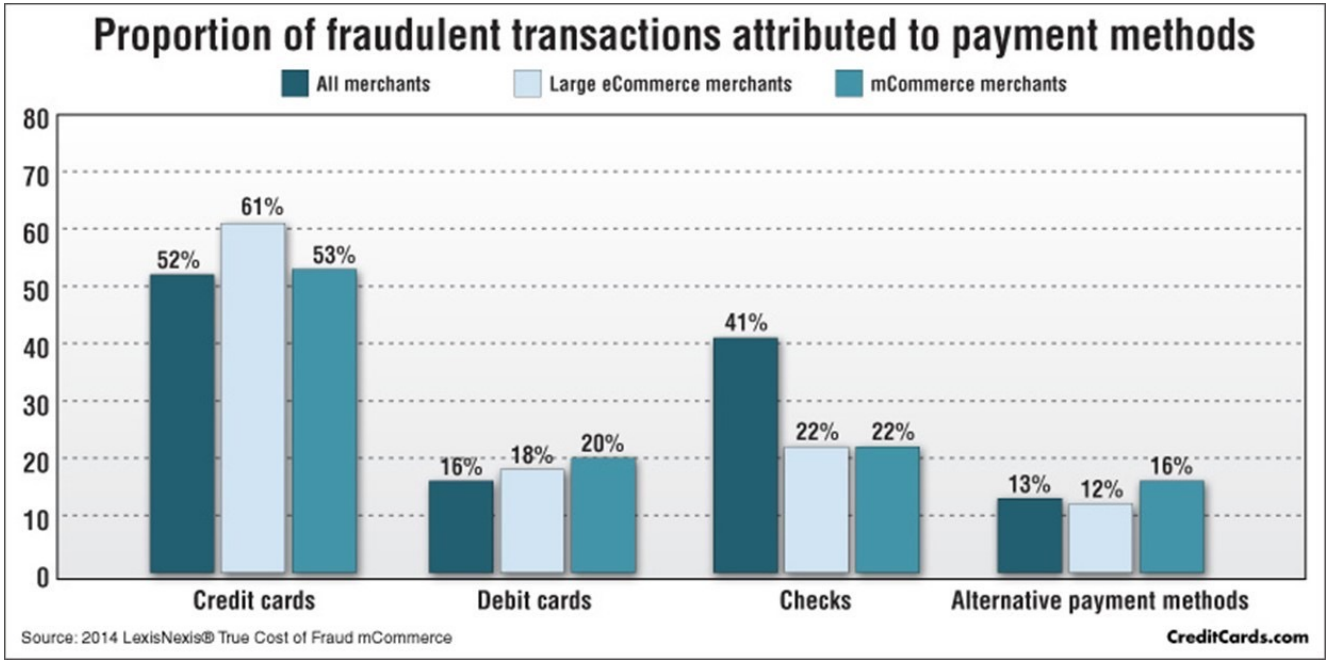
3.4. Rủi ro trong thanh toán

Figure 9: Top 3 Payment Types with Highest Number of Fraud Attempts
(by % of Non-Financial Services Respondents)



Q15: Indicate the payment types where your organization experienced the highest number of fraud attempts (regardless of actual financial losses) in 2013. (Select and rank up to three that are highest.)

3.4. Rủi ro trong thanh toán



❸ Phân loại rủi ro theo tiến trình kinh doanh TMĐT

Phân loại rủi ro trong thanh toán

- **Rủi ro xuất trình thẻ thanh toán (Clear and present risk)**: RR xảy ra khi thông tin chi tiết của khách hàng, như số thẻ bị đánh cắp khi thẻ được xuất trình cho thanh toán tại các quầy thanh toán của nhà hàng, cửa hàng bán lẻ và máy ATM.
- **Đe dọa ẩn (Hidden threats)**: RR xảy ra trong quá trình thành toán trực tuyến, qua thư điện tử, điện thoại hoặc fax.

❸ Phân loại rủi ro theo tiến trình kinh doanh TMĐT

Phân loại rủi ro trong thanh toán

- **Intercept/mail non-receipt fraud**: Điều này xảy ra khi đổi thẻ hay thẻ mới của chủ thẻ bị đánh cắp trước khi được chuyển tới chủ thẻ. Ví dụ, việc sử dụng các hộp thư ngoài cổng, không chuyển thư trực tiếp đến tay chủ thẻ đã tạo ra các lỗ hổng cho loại gian lận này.
- **Thẻ giả mạo/nhân bản (Skimming/cloning/counterfeit cards)**: Các dải từ của thẻ chứa thông tin mà kẻ lừa đảo cần lấy được.

❸ Phân loại rủi ro theo tiến trình kinh doanh TMĐT

Phân loại rủi ro trong thanh toán

- **ATM skimming:** cũng giống như hành vi trộm cắp danh tính thẻ ghi nợ, kẻ trộm sử dụng thiết bị điện tử ẩn để lấy cắp các thông tin cá nhân được lưu trữ trên thẻ của chủ thẻ và lấy cắp số PIN để truy cập vào tài khoản của chủ thẻ. Skimming thẻ gồm 2 việc:
- Phần đầu tiên là skimmer chính nó, một đầu đọc thẻ được đặt trên khe cắm thẻ thực sự của máy ATM. Khi trượt thẻ vào máy ATM, chủ thẻ không biết đang trượt thẻ thông qua đầu đọc giả, thiết bị scans và lưu trữ tất cả các thông tin trên dải từ.

❸ Phân loại rủi ro theo tiến trình kinh doanh TMĐT

Phân loại rủi ro trong thanh toán

Để truy cập vào tài khoản trên một máy ATM, kẻ trộm cần có số PIN.

- Bằng cách đặt máy ảnh đi kèm trong - ẩn trên hoặc gần các máy ATM, máy ảnh gián điệp nhỏ được định vị để có được một cái nhìn rõ ràng của bàn phím và ghi lại tất cả các hành động số PIN của ATM.
- Một số chương trình ATM skimming sử dụng bàn phím giả thay cho máy ảnh để chụp số PIN. Cũng giống như card skimmer được đặt khít (fit over) vào khe cắm thật của máy ATM, bàn phím lướt skimming được thiết kế để ngụy trang (như một chiếc bao găng tay).
- Có thể đánh cắp thông tin thẻ mà không cần skimming.

❸ Phân loại rủi ro theo tiến trình kinh doanh TMĐT

Phân loại rủi ro trong thanh toán

Các PP sử dụng ***keystroke logging***:

- Sử dụng phần cứng và phần mềm
- Phân tích dải băng điện tử (electromagnetic analysis)
- Phân tích âm (acoustic analysis).
- Phishing

❸ Phân loại rủi ro theo tiến trình kinh doanh TMĐT

Phân loại rủi ro trong thanh toán

Để truy cập vào tài khoản trên một máy ATM, kẻ trộm cần có số PIN.

- Bằng cách đặt máy ảnh đi kèm trong - ẩn trên hoặc gần các máy ATM, máy ảnh gián điệp nhỏ được định vị để có được một cái nhìn rõ ràng của bàn phím và ghi lại tất cả các hành động số PIN của ATM.
- Một số chương trình ATM skimming sử dụng bàn phím giả thay cho máy ảnh để chụp số PIN. Cũng giống như card skimmer được đặt khít (fit over) vào khe cắm thật của máy ATM, bàn phím lướt skimming được thiết kế để ngụy trang (như một chiếc bao găng tay).
- Có thể đánh cắp thông tin thẻ mà không cần skimming.

Phân loại rủi ro trong thương mại điện tử

Theo nguồn phát sinh rủi ro	Theo tiến trình kinh doanh TMĐT	Theo đối tượng chịu tác động
Rủi ro khách quan Rủi ro chủ quan	Rủi ro thị trường Rủi ro từ khách hàng Rủi ro từ nhà cung ứng Rủi ro trong vận chuyển Rủi ro trong giao nhận hàng Rủi ro trong thanh toán	Rủi ro về dữ liệu Rủi ro về công nghệ Rủi ro về các thủ tục quy trình giao dịch Rủi ro về luật pháp và quy trình công nghệ

❹ Rủi ro đối với các tác nhân còn lại …

4.1. Rủi ro đối với mua hàng trực tuyến

- Người mua bị hạn chế trong công tác xác thực hàng hóa hay dịch vụ: không được kiểm tra hàng hóa trước khi thanh toán.
- Mua phải hàng kém chất lượng, hàng đến chậm
- Hàng hóa nhận được không đáp ứng kì vọng, Giao nhận các hàng hóa vật thể, hữu hình: không tương đồng như mô tả, khuyết tật.

❹ Rủi ro đối với các tác nhân còn lại …

4.1. Rủi ro đối với mua hàng trực tuyến

- RR chủ sở hữu thẻ thanh toán: Để lộ mã số bí mật (PIN) đồng thời làm mất thẻ mà chưa kịp báo cho ngân hàng phát hành thẻ.
- Bẫy mạng lưới đa cấp: bán hàng đa cấp TMĐT – trường hợp MB24,
- Mua hàng từ website nước ngoài, các rủi ro có nguồn gốc từ thay đổi chính sách, quy định pháp luật – trường hợp đầu tư vào Bitcoin.

❹ Rủi ro đối với các tác nhân còn lại …

4.2. Rủi ro đấu giá, đầu thầu trực tuyến

- Theo thống kê NW3C/FBI 2007 chỉ ra rằng gian lận đấu giá trực tuyến là loại vi phạm phổ biến nhất đã báo cáo cho Trung tâm Khiếu nại tội phạm Internet. Trong số 207.492 khiếu nại giữa 1/1 đến 31/12/2020, gian lận đấu giá trực tuyến chiếm 45% của 86.279 trường hợp được đề cập tới các cơ quan thực thi pháp luật của Mỹ và chiếm 33% giá trị tổn thất.
- Cả người mua và người bán (thương nhân) đều có thể trở thành nạn nhân của gian lận đấu giá trực tuyến. Một số cách thức diễn ra trong hoặc sau các đấu giá trực tuyến.

❹ Rủi ro đối với các tác nhân còn lại …

4.2. Rủi ro đấu giá, đầu thầu trực tuyến

Các cách thức mà các cuộc đấu giá trực tuyến có thể bị khai thác hoặc sử dụng bởi các nhà đấu giá và nhà thầu như sau (Adams 2006; Boyd & mao 2000):

❹ Rủi ro đối với các tác nhân còn lại …

4.2. Rủi ro đấu giá, đầu thầu trực tuyến

❹ Rủi ro đối với các tác nhân còn lại …

Nhận biết rủi ro đấu giá

Hàng hóa thị trường chợ đen (Black market goods). The seller offers goods that are stolen and/or copied (e.g., software, music CDs, and videos). Often they arrive with no warranty, instructions, or box.

❹ Rủi ro đối với các tác nhân còn lại …

4.3. Rủi ro khởi nghiệp kinh doanh điện tử

Các lưu ý đ/v dự án kinh doanh TMĐT

- Ý tưởng kinh doanh TMĐT liệu có khả thi
- Chi phí đầu tư ban đầu
- Ai đầu tư
- Tổ chức quản lý ntn?
- Chi phí vận hành,
- Chi phí quảng cáo;
- Thị trường
- Lợi nhuận, thời gian hòa
- Triển vọng

❹ Rủi ro đối với các tác nhân còn lại …

4.3. Rủi ro khởi nghiệp kinh doanh điện tử

Khó khăn

- Vạn sự khởi đầu nan!!! Tay trắng dựng nghiệp. Thiếu kinh nghiệm, kiến thức, vốn, nhưng nhiều mạo hiểm = high risk ➔ dễ đổ vỡ, thất bại
- Dự báo không chính xác nhu cầu thị trường
- Vi phạm các quy định pháp luật
- Thiếu kinh nghiệm quản lý, hợp tác, cộng sự: liên kết lỏng lẻo, xung đột, mâu thuẫn trong quản lý.
- Áp lực thời gian: thời gian để thuyết phục nhà đầu tư mạo hiểm.
- Mất sản nghiệp, trắng tay, kể cả phạm tội

❹ Rủi ro đối với các tác nhân còn lại …

4.3. Rủi ro khởi nghiệp kinh doanh điện tử

Ví dụ: Vụ Nguyễn Hà Đông và Điều 292 BLHS

Cộng đồng start-up lo thành tội phạm vì luật mới

Việc nêu tên một số dịch vụ liên quan đến nhiều start-up hiện nay trong Bộ Luật hình sự khiến cộng đồng khởi nghiệp lo lắng về khả năng vi phạm pháp luật, song cũng có ý kiến chuyên gia cho rằng cần có cách hiểu chính xác về quy định trên.

Điều 292. Tội cung cấp dịch vụ trái phép trên mạng máy tính, mạng viễn thông

1. Người nào cung cấp một trong các dịch vụ sau đây trên mạng máy tính, mạng viễn thông mà chưa được phép của cơ quan nhà nước có thẩm quyền theo quy định của pháp luật không có giấy phép hoặc không đúng nội dung được cấp phép và thu lợi bất chính từ 100.000.000 đồng đến dưới 300.000.000 đồng, 50.000.000 đồng đến dưới 200.000.000 đồng hoặc có doanh thu từ 500.000.000 đồng đến dưới 2.000.000.000 đồng thì bị phạt tiền từ 200.000.000 đồng đến 500.000.000 đồng hoặc phạt cải tạo không giam giữ đến 02 năm:

a) Kinh doanh vàng miếng trên tài khoản;

b) Sàn giao dịch thương mại điện tử;

c) Kinh doanh đa cấp;

d) Trung gian thanh toán;

đ) Trò chơi điện tử trên mạng;

PA1: Liệt kê cụ thể các dịch vụ khác trên mạng máy tính, mạng viễn thông.

PA2: Bỏ điểm này.

2. Phạm tội thuộc một trong các trường hợp sau đây thì bị phạt tiền từ 500.000.000 đồng đến 1.500.000.000 đồng hoặc phạt tù từ 03 tháng đến 02 năm:

đ) Thu lợi bất chính 200.000.000-300.000.000 đồng đến dưới 500.000.000 đồng hoặc có doanh thu từ 2.000.000.000 đồng đến dưới 5.000.000.000 đồng.

3. Phạm tội trong trường hợp thu lợi bất chính 500.000.000 đồng trở lên hoặc có doanh thu 5.000.000.000 đồng trở lên thì bị phạt tiền từ 1.500.000.000 đồng đến 5.000.000.000 đồng hoặc bị phạt tù từ 02 năm đến 05 năm.

❹ Rủi ro đối với các tác nhân còn lại …

4.4. Rủi ro trên mạng xã hội

- Người dùng SM có thể bị rò rỉ thông tin cá nhân, thông tin kinh doanh vô ý hoặc sơ ý. Ví dụ, một hình ảnh chụp được đăng tải ngay có thể gợi ý thông tin cá nhân về địa điểm người dùng đang ở đâu; hoặc những thông tin cá nhân khác được khai thác (điện thoại, gia đình, nghề nghiệp…)
- Người dùng SM có thể gửi các nội dung *racially or sexually offensive content*, phỉ báng, nói xấu cá nhân, tổ chức sử dụng các phương tiện SM để vi phạm pháp luật, chính sách sử dụng của trang mạng xã hội, vi phạm bí mật riêng tư.
- Một số nội dung phương tiện truyền thông xã hội tạo thành hồ sơ kinh doanh phải được bảo quản phù hợp với yêu cầu lưu giữ công ty, và quy định pháp luật, nhưng điều đó có thể không được lưu trữ một cách thích hợp.
- Địa điểm để phát tán các mã độc, virus.

3

Các khía cạnh an ninh trong thương mại điện tử

Các khía cạnh của an toàn thông tin

- ITU-T là cụm từ viết tắt của International Telecommunication Union - Telecommunication Standardization Sector là lĩnh vực Tiêu chuẩn viễn thông - thuộc Tổ chức Viễn thông quốc tế.

- Theo ITU-T X.800, ATTT bao gồm ba khía cạnh (aspects):

  - Tấn công (security attack);
  - Dịch vụ bảo mật (security service),
  - Cơ chế bảo mật, an toàn (security mechanism)

Các khía cạnh của an toàn thông tin

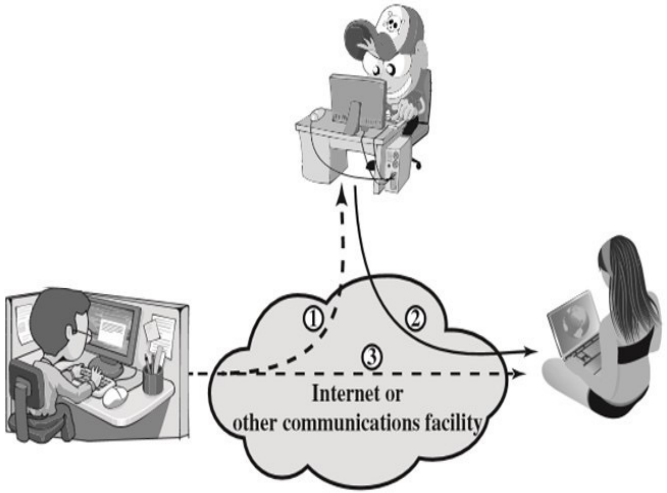
Tấn công: Bất kỳ hành động nào làm ảnh hưởng hoặc tác

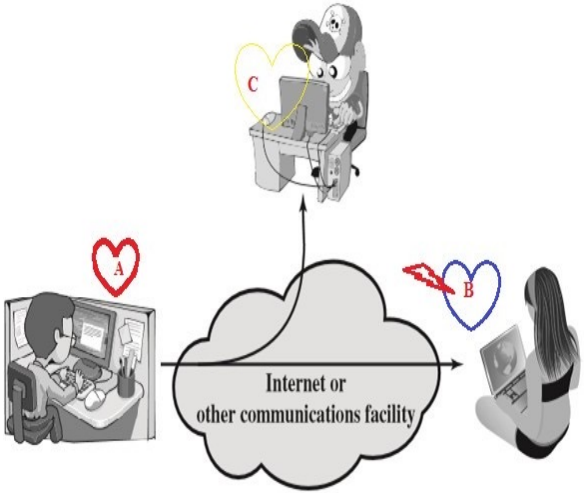
động tới ATTT. Nhiều loại khác nhau của các cuộc tấn công, có thể được phân loại: tấn công thụ động Passive attacks các cuộc tấn chủ động Active attacks

Dịch vụ bảo mật: Bảo vệ dữ liệu không bị tiết lộ trái phép, bảo đảm tính toàn vẹn, chống chối bỏ , kiểm soát truy cập, bảo đảm tính sẵn sàng ….

Các cơ chế bảo mật: Phương tiện để thực hiện các dịch vụ bảo mật: Mã hóa: Mã hóa đối xứng, Mã hóa khóa công khai, Quản lý chìa; Hàm băm; Các mã xác thực thông điệp; Chữ ký số; Các giao thức xác thực thực thể

Mối liên quan kiểu tấn công và khía cạnh an toàn TT





Các khía cạnh an ninh trong thương mại điện tử

Tính toàn vẹn: nghĩa là dữ liệu không bị chỉnh sửa, nó khác với tính toàn vẹn trong tham chiếu của cơ sở dữ liệu, mặc dù nó có thể được xem như là một trường hợp đặc biệt của tính nhất quán như được hiểu trong mô hình cổ điển ACID (tính nguyên tử atomicity), tính nhất quán (consistency), tính cách ly (isolation), tính lâu bền (durability) – là một tập các thuộc tính cơ sở dữ liệu đáng tin cậy) của xử lý giao dịch bị xâm hại khi một thông điệp bị chỉnh sửa trong giao dịch. Hệ thống TMĐT an toàn luôn cung cấp các thông điệp toàn vẹn và bí mật.

Các khía cạnh an ninh trong thương mại điện tử

Tính sẵn sàng: Mọi hệ thống TMĐT đều có mục đích riêng và thông tin phải luôn luôn sẵn sàng khi cần thiết. Điều đó có nghĩa rằng hệ thống tính toán sử dụng để lưu trữ và xử lý thông tin, có một hệ thống điều khiển bảo mật sử dụng để bảo vệ nó, và kênh kết nối sử dụng để truy cập nó phải luôn hoạt động chính xác. Hệ thống có tính sẵn sàng cao hướng đến sự sẵn sàng ở mọi thời điểm, tránh được những rủi ro cả về phần cứng, phần mềm như: mất điện, hỏng phần cứng, cập nhật, nâng cấp hệ thống…Đảm bảo tính sẵn sàng cũng có nghĩa là tránh được tấn công từ chối dịch vụ.

Các khía cạnh an ninh trong thương mại điện tử

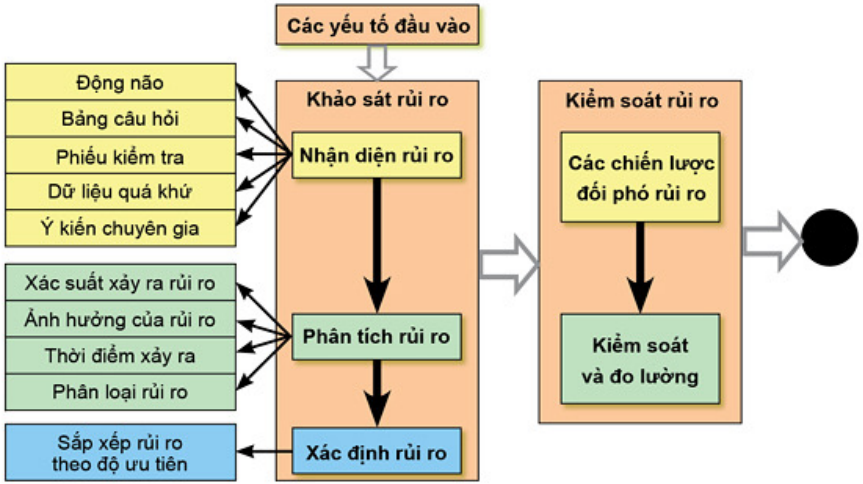
Tính chống chối bỏ (phủ nhận) có nghĩa rằng một bên giao dịch không thể phủ nhận việc họ đã thực hiện giao dịch với các bên khác. Ví dụ: trong khi giao dịch mua hàng qua mạng, khi khách hàng đã gửi số thẻ tín dụng cho bên bán, đã thanh toán thành công, thì bên bán không thể phủ nhận việc họ đã nhận được tiền, (trừ trường hợp hệ thống không đảm bảo tính ATTT trong giao dịch).

Các khía cạnh an ninh trong thương mại điện tử

Tính xác thực: Trong hoạt động tính toán, kinh doanh qua mạng và an toàn thông tin, tính xác thực là vô cùng cần thiết để đảm bảo rằng dữ liệu, giao dịch, kết nối hoặc các tài liệu (tài liệu điện tử hoặc tài liệu cứng) đều là xác thật (genuine). Nó cũng quan trọng cho việc xác nhận rằng các bên liên quan biết họ là ai trong hệ thống.

CASE STUDY 1

Quản trị rủi ro trong dự án phần mềm



CASE STUDY 2

Rủi ro khi mở phòng net

CASE STUDY 3

Rủi ro khi kinh doanh online

VIRUS

Xuất hiện lần đầu tiên vào năm 1983. Virus là một chương trình máy tính có khả năng tự nhân bản và lan tỏa. Mức độ nghiêm trọng của virus dao động khác nhau tùy vào chủ ý của người viết ra virus:

- Ít nhất virus cũng chiếm tài nguyên máy tính và làm tốc độ xử lý của máy tính chậm đi
- nghiêm trọng hơn, virus có thể xóa file, format lại ổ cứng hoặc gây những hư hỏng khác.

Trước kia virus chủ yếu lan tỏa qua việc sử dụng chung file, đĩa mềm...

Ngày nay trên môi trường Internet, virus có cơ hội lan tỏa rộng hơn, nhanh hơn.

Virus đa phần được gửi qua email, ẩn dưới các file gửi kèm (attachment) và lây nhiễm trong mạng nội bộ các doanh nghiệp, làm doanh nghiệp phải tốn kém thời gian, chi phí, hiệu quả, mất dữ liệu...

Cho đến nay hàng chục nghìn loại virus đã được nhận dạng và ước tính mỗi tháng có khoảng 400 loại virus mới được tạo ra.

Sâu máy tính (worms)

Sâu máy tính khác với virus ở chỗ sâu máy tính không thâm nhập vào file mà thâm nhập vào hệ thống.

Ví dụ:

- Sâu mạng (network worm) tự nhân bản trong toàn hệ thống mạng.
- Sâu Internet tự nhân bản và tự gửi chúng qua hệ thống Internet thông qua những máy tính bảo mật kém.
- Sâu email tự gửi những bản nhân bản của chúng qua hệ thống email.

Trojan

Đặt tên theo truyền thuyết con ngựa Trojan của thành Troy.

Là một loại chương trình nguy hiểm (malware) được dùng để thâm nhập vào máy tính mà người sử dụng máy tính không hay biết. Không giống như virus, Trojan không tự nhân bản được.

Người sử dụng máy tính bị nhiễm Trojan có thể bị đánh cắp mật khẩu, tên tài khoản, số thẻ tín dụng và những thông tin quan trọng khác.

- Có thể cài đặt chương trình theo dõi bàn phím (keystroke logger) để lưu lại hết những phím đã được gõ rồi sau đó gửi "báo cáo" về cho một địa chỉ email được định trước
- Gửi email với nội dung khuyến cáo người sử dụng nên click vào một đường link cung cấp trong email để đến một website nào đó

Phishing attacks

Xuất hiện từ năm 1996

Mưu đồ sử dụng email, tin nhắn dạng pop-up hay các trang web để đánh lừa người dùng cung cấp các thông tin nhạy cảm

- Lấy cắp thông tin quan trọng
- Thẻ tín dụng => mất tiền

Tạo ra những website bán hàng, bán dịch vụ “y như thật” trên mạng và tối ưu hóa chúng trên Google để “nạn nhân” tự tìm thấy và mua hàng/dịch vụ trên những website này

CHƯƠNG 3

Giải pháp mang tính kỹ thuật đối phó với rủi ro trong thương mại điện tử

NỘI DUNG

1. Nhận biết rủi ro trong TMĐT
2. Phân tích rủi ro trong TMĐT
3. Đánh giá mối đe dọa của rủi ro trong TMĐT

1

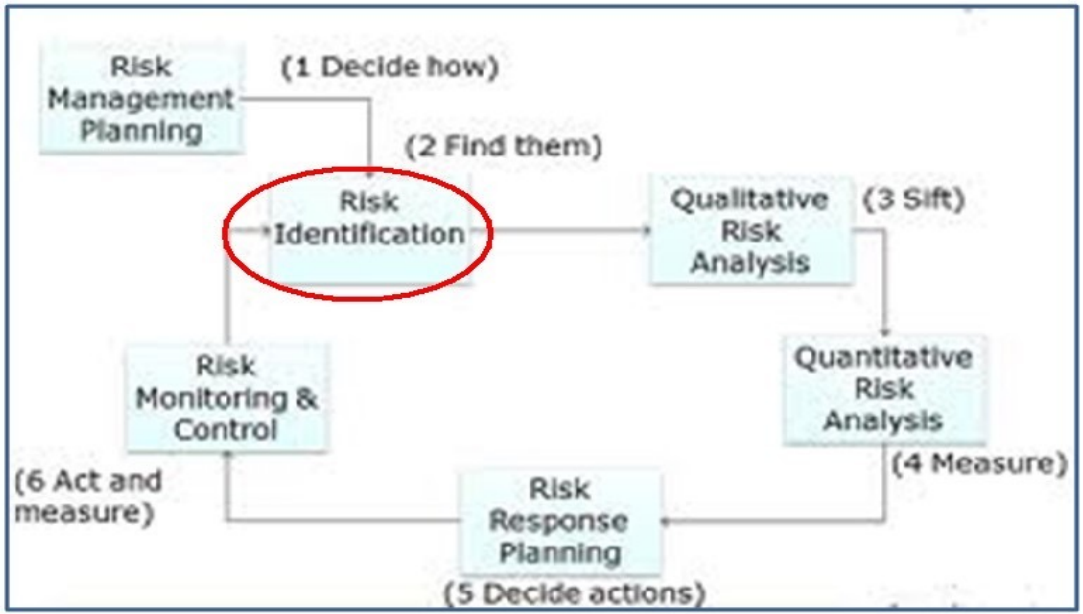
Nhận biết rủi ro

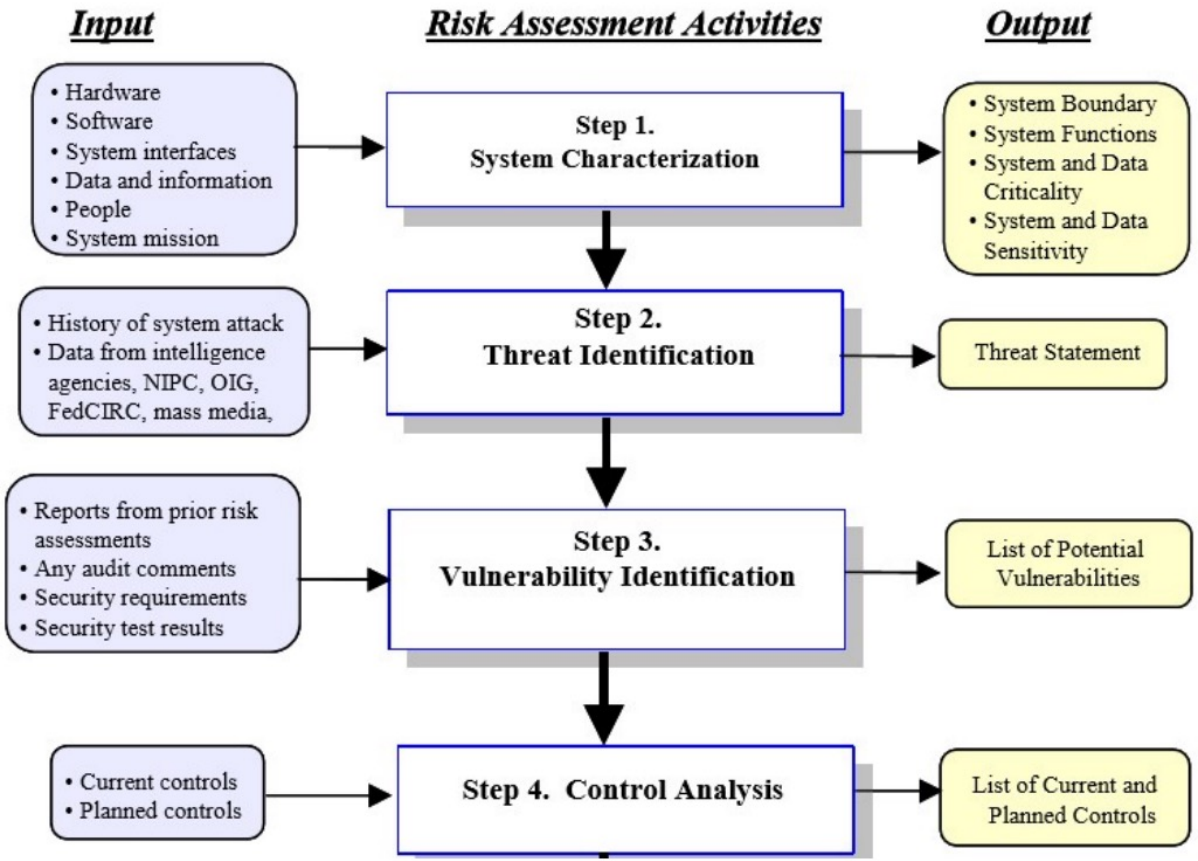
Ý nghĩa của việc nhận biết RR TMĐT

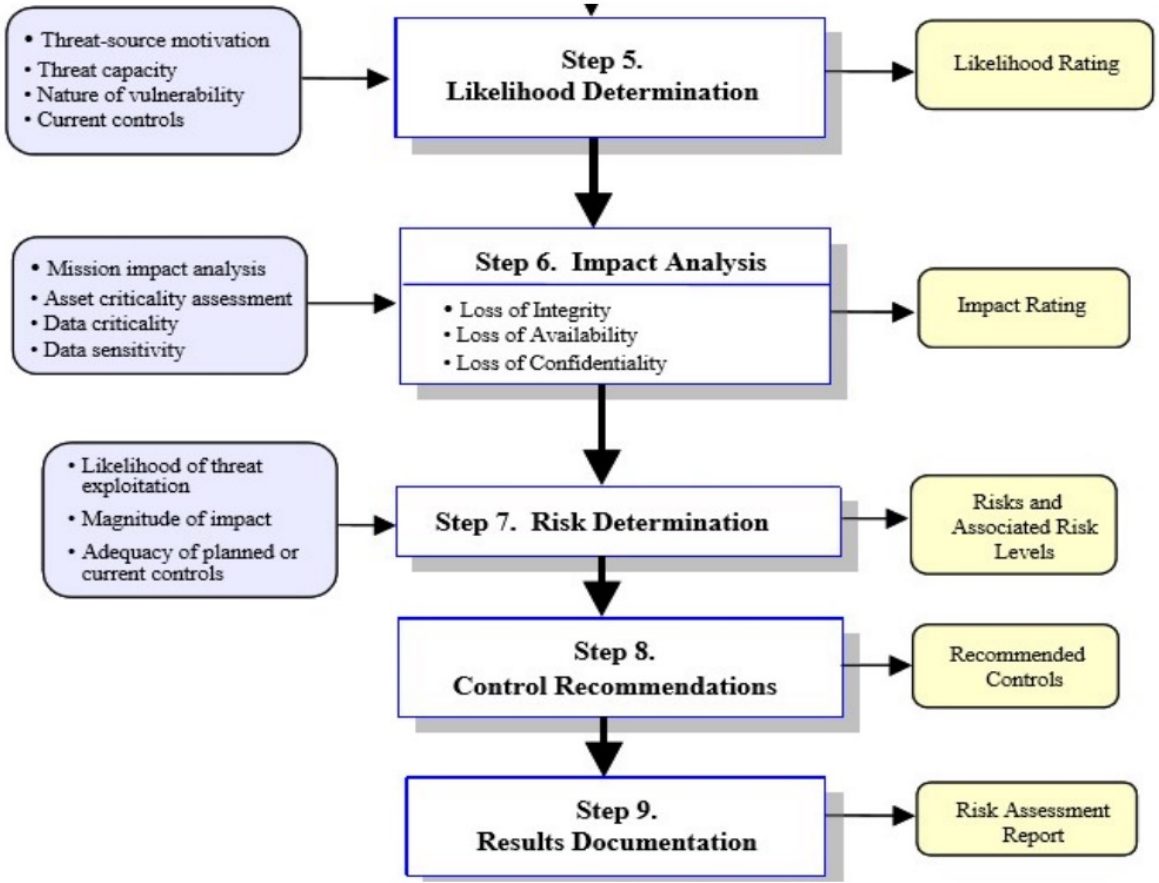
Nhận biết rủi ro là cốt lõi của quá trình QTRR. Nhận biết rủi ro giúp nhà quản trị chủ động quản trị rủi ro, đánh giá mức độ rủi ro, chủ động thực hiện các biện pháp bảo vệ phòng ngừa hiệu quả, đúng lúc, tối thiểu hóa chi phí.

- Nhận biết RR thông tin TMĐT là nhận biết các đe dọa, tấn công, lỗ hổng ATTT.
- Nếu một đe dọa không được nhận biết nó không thể được kiểm soát. Một lỗ hổng không được phát hiện sớm, được vá, một tấn công không được đối phó, sẽ có những tác động xấu tới các mục tiêu của DN

Cách thức tiếp cận nhận biết rủi ro TMĐT như thế nào?




Input
Risk Assessment Activities
Output
• Hardware
• Software
• System interfaces
• Data and information
• People
• System mission
Step 1.
System Characterization
• System Boundary
• System Functions
• System and Data Criticality
• System and Data Sensitivity
• History of system attack
• Data from intelligence agencies, NIPC, OIG, FedCIRC, mass media,
Step 2.
Threat Identification
Threat Statement
• Reports from prior risk assessments
• Any audit comments
• Security requirements
• Security test results
Step 3.
Vulnerability Identification
List of Potential Vulnerabilities
• Current controls
• Planned controls
Step 4. Control Analysis
List of Current and Planned Controls


• Threat-source motivation
• Threat capacity
• Nature of vulnerability
• Current controls
Step 5.
Likelihood Determination
Likelihood Rating
• Mission impact analysis
• Asset criticality assessment
• Data criticality
• Data sensitivity
Step 6. Impact Analysis
• Loss of Integrity
• Loss of Availability
• Loss of Confidentiality
Impact Rating
• Likelihood of threat exploitation
• Magnitude of impact
• Adequacy of planned or current controls
Step 7. Risk Determination
Risks and Associated Risk Levels
Step 8.
Control Recommendations
Recommended Controls
Step 9.
Results Documentation
Risk Assessment Report

Các khái niệm liên quan nhận biết rủi ro TMĐT

Nhận biết rủi ro (Risk Identification): là liệt kê các RR mà DN, KH có thể gặp phải và đánh giá (sơ bộ) mức độ xảy ra của chúng. Đây là bước tiếp sau xây dựng kế hoạch QTRR.

Nhận biết RR thông tin trong TMĐT bao gồm nhận biết các đe dọa an toàn (security threats) và + xác định các lỗ hổng bảo mật/an toàn (computing vulnerabilities).

Các khái niệm liên quan nhận biết rủi ro TMĐT

Khái niệm đe dọa an toàn

Đe dọa (threat): theo nghĩa rộng

- là các nguồn nguy hiểm;
- bất kì lực lượng đối lập,
- điều kiện, nguồn hoặc tình huống

=> có khả năng ảnh hướng tới thực hiện/phá vỡ KH hoặc làm giảm khả năng thực hiện nhiệm vụ, KH.

Khái niệm đe dọa an toàn

Đe dọa an toàn (security threats): Trong an toàn máy tính, đe dọa là một mối nguy hiểm có thể bị khai thác từ một lỗ hổng để xâm phạm HT thông tin và gây ra các thiệt hại, mất an toàn.

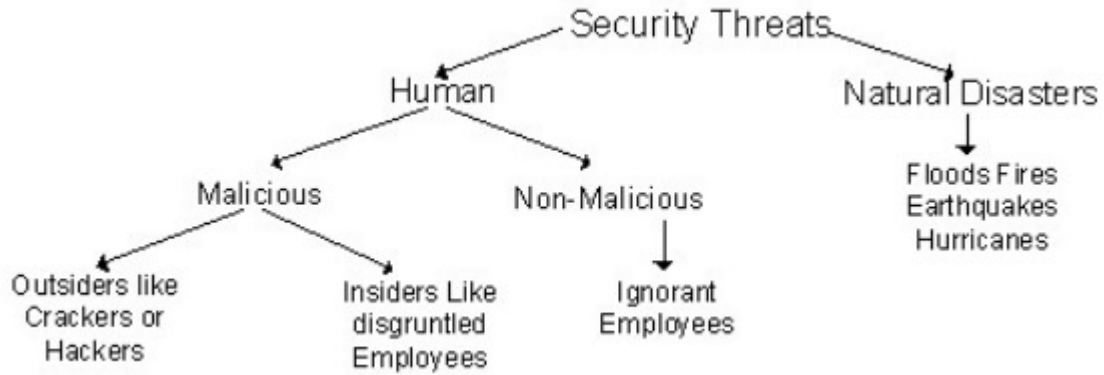
Nguồn đe dọa:

• Khi có một hoàn cảnh, một khả năng, một hành động hay một sự kiện mà có thể có điều kiện vi phạm để gây hại (khả năng xảy ra)

• Có thể do chủ ý của con người (phát tán virus máy tính) hoặc sự cố bất khả kháng (động đất, sóng thần…)

Nguồn đe dọa (tiếp…)

- Tổ chức tội phạm,
- Phần mềm gián điệp, phần mềm độc hại,
- Các công ty phần mềm quảng cáo,
- Các nhân viên nội bộ bất bình bắt đầu tấn công sử dụng lao động của họ.
- Sâu máy tính và virus cũng đặc trưng cho một mối đe dọa khi chúng có thể có thể gây ra thiệt hại bằng cách lây nhiễm các máy móc và gây thiệt hại tự động



1.2. Các phương pháp nhận diện rủi ro chủ yếu

❶ ***Sử dụng mẫu Bảng hỏi phân tích rủi ro***

- Nội dung của phương pháp
- Ưu điểm: các câu hỏi được sắp xếp theo chủ đề, dễ hiểu
- Hạn chế: mất thời gian và chi phí thu thập thông tin; khó nhận dạng tất cả các rủi ro (nhất là rủi ro đặc trưng), khó tìm kiếm các thông tin bổ sung

1.2. Các phương pháp nhận diện rủi ro chủ yếu

❷ ***Phân tích các báo cáo tài chính***

- Nội dung của phương pháp
- Phân tích sự biến động của các tài khoản, các báo cáo hoạt động kinh doanh, bảng cân đối kế toán, các chỉ tiêu tài chính và các tài liệu bổ trợ.
- Ưu điểm: Xác định được nhiều loại rủi ro, dễ hiểu, dễ thực hiện, có tính tin cậy cao, khách quan, rõ ràng
- Hạn chế: Khó phát hiện các rủi ro đặc thù, rủi ro mới, và các đối tượng có nguy cơ rủi ro cụ thể

1.2. Các phương pháp nhận diện rủi ro chủ yếu

❸ *Kiểm tra thực tế và làm việc trực tiếp với các bộ phận/ các hệ thống liên quan*

Nội dung của phương pháp

Điều kiện thực hiện:

+ Sự hợp tác của các bộ phận khác

+ Quy định về trách nhiệm rõ ràng

1.2. Các phương pháp nhận diện rủi ro chủ yếu

❹ ***Nghiên cứu các số liệu tổn thất trong quá khứ***

- Nội dung của phương pháp: Phân tích các hồ sơ lưu trữ số liệu (dữ liệu) về rủi ro và những tổn thất đã xảy ra
- Ưu điểm: Cung cấp thông tin đầy đủ về tất cả các rủi ro đã từng xảy ra
- Hạn chế: Khó phát hiện rủi ro mới

2

Phân tích rủi ro (Risk Analysis)

2. Phân tích rủi ro (Risk Analysis)

- Là thực hiện đánh giá toàn diện và chi tiết các RR tiềm ẩn và các lỗ hổng bảo mật, tính toàn vẹn, tính sẵn sàng của các thông tin…
- Là việc xác định, đánh giá và xếp hạng các RR với mục đích tiết kiệm các nguồn lực cũng như giảm thiểu kiểm soát, tổn thất và tác động không mong muốn và tối đa hóa việc thực hiện các cơ hội.

2. Phân tích rủi ro (Risk Analysis)

Quy trình phân tích rủi ro

- Xác định phạm vi, mục tiêu các đối tượng cần bảo vệ (Map Objectives)
- Nhận biết các đe dọa, tấn công (ID threats)
- Đánh giá lỗ hổng (Assess Vulnerabilities)
- Xác định xác suất xảy ra (Determine Risk Likelihood
- Xác định tổn hại (Determine Threat Impact)
- Xác định cấp độ RR (Determine Level or Risk)
- Lập hồ sơ (Documentation)

2. Phân tích rủi ro (Risk Analysis)

❶ PP định tính phân tích RR

Theo tần xuất xuất hiện của RR: có 4 mức qua ước lượng sự quan trọng của nó.

- Mức thường xuyên
- Mức hay xảy ra
- Mức đôi khi, thỉnh thoảng
- Mức hiếm (ít) khi

2. Phân tích rủi ro (Risk Analysis)

❶ PP định tính phân tích RR

Theo thời điểm xuất hiện/xảy ra: có 4 mức để ước lượng thời điểm rủi ro xuất hiện, tùy sự tác động của nó.

- Mức ngay lập tức
- Mức rất gần
- Mức sắp xảy ra
- Mức rất lâu

2. Phân tích rủi ro (Risk Analysis)

❷ Các nguyên tắc phân tích RR theo OWASP

OWASP (The Open Web Application Security Project) đề xuất các nguyên tắc phân tích RR, mức điểm từ 0 - 9, với đánh giá xác suất xảy ra trên hai yếu tố:

1. Yếu tố đe dọa:

Mức độ kĩ năng đe dọa (Skill level): nhóm đe dọa có kĩ năng đe dọa như thế nào?

Không có kĩ năng (1)

Một số kĩ năng (3)

Có nhiều kĩ năng dùng máy tính (4)

Kĩ năng lập trình và mạng (6)

Kĩ năng truy nhập bảo mật (9)

❷ Các nguyên tắc phân tích RR theo OWASP

1. Yếu tố đe dọa:

Động cơ (Motive): của phát hiện, tìm ra lỗ hổng là gì?

- Không vì được phần thưởng, lợi ích (1)
- Có thể được phần /khen thưởng (4)
- Được khen thưởng, vụ lợi (9)

Cơ hội, thời cơ (Opportunity): những nguồn lực và cơ hội nào cần thiết để tấn công khai thác lỗ hổng xảy ra

- Tiếp cận hoàn toàn các nguồn lực được yêu cầu (0)
- Tiếp cận đặc biệt các nguồn lực yêu cầu (4)
- Tiếp cách lẻ tẻ các nguồn lực yêu cầu (7)
- Không thể tiếp cận các nguồn lực yêu cầu (9)

❷ Các nguyên tắc phân tích RR theo OWASP

1. Yếu tố đe dọa:

Quy mô (Size): Nhóm đe doạ lớn đến mức nào?

- Người phát triển (2)
- Hệ thống hành chính (2)
- Users nội bộ (4)
- Đối tác (5)
- Users thật (6)
- Người dùng internet ẩn danh (9)

❷ Các nguyên tắc phân tích RR theo OWASP

2. Yếu tố lỗ hổng (Vulnerability factors)

Nhận thức (Awareness):

- Không xác định (1)
- Giấu kín (4)
- Hiển nhiên (6)
- Biết rộng rãi (9)

Phát hiện xâm nhập (Intrusion detection):

- Xâm nhập sâu (1)
- Đã đăng nhập và xem xét (3)
- Đã đăng nhập nhưng chưa xem xét(8)
- Chưa đăng nhập (9)

2. Phân tích rủi ro (Risk Analysis)

❸ Phân tích RR theo mức độ

Đánh giá tổn thất theo thang điểm từ 0 – 9

Tổn thất về kĩ thuật: được xem xét là: tính bảo mật C, tính sẵn sàng A và tính toàn vẹn I. Mục đích là ước tính độ lớn trên hệ thống nếu lỗ hổng bị khai thác.

Tổn thất tính bảo mật: Dữ liệu bị tiết lộ, và dữ liệu nhạy cảm.

Dữ liệu bị tiết lộ rất nhỏ (2)

Dữ liệu quan trọng bị tiết lộ rất nhỏ (6)

Dữ liệu bị tiết lộ mở rộng (6)

Dữ liệu quan trọng bị tiết lộ mở rộng (7)

Tất cả dữ liệu bị tiết lộ (9)

❸ Phân tích RR theo mức độ

Tổn thất tính toàn vẹn: Bao nhiêu dữ liệu bị chiếm giữ và thiệt hại?

Một số dữ liệu bị chiếm giữ (1)
Một số dữ liệu quan trọng bị chiếm giữ (3)
Một số lớn dữ liệu bị chiếm giữ (5)
Một số lớn dữ liệu quan trọng bị chiếm giữ (7)
Tất cả dữ liệu bị chiếm giữ (9)

Tổn thất tính sẵn sàng: Bao nhiêu dịch vụ bị mất và mức quan trọng của dịch vụ đó?

Một số DV bổ sung bị gián đoạn (1)
Một số DV chủ yếu bị gián đoạn (5)
Các DV bổ sung bị gián đoạn mở rộng (5)
Các DV chính bị gián đoạn mở rộng (7)
Tất cả các DV bị đứt, ngưng (9)

❸ Phân tích RR theo mức độ

Giá trị tài sản	Giá trị C+I+A
Thấp (1)	1-3
Trung bình (2)	4-6
Cao (3)	7-9
Rất cao (4)	10-12
Cực cao (5)	13-15

❸ Phân tích RR theo mức độ Mô hình DREAD

- Thiệt hại (Damage_D1)
- Khả năng tái tạo (Reproductivity_R)
- Khả năng khai thác (Exploitability_E)
- Người bị ảnh hưởng (Affected Users_A)
- Khả năng phát hiện (Discoverability_ D2)

❸ Phân tích RR theo mức độ

Tác động:

- Damage (D1)
- Người bị ảnh hưởng (A)

Xác suất xảy ra:

- R
- E
- D2

❸ Phân tích RR theo mức độ

Tác động:

- Damage (D1)= C+I+A
- Người bị ảnh hưởng: được phân thành 5 nhóm

➢ Quản trị viên

➢ Người dùng cấp cao

➢ Nhóm

➢ User

➢ Công chúng

❸ Phân tích RR theo mức độ

Xác Suất xảy ra:

- Khả năng tái tạo_ R: gồm 3 mức độ
  - ➢ KHó tái tạo ngay cả khi có kiến thức về lỗ hổng bảo mật
  - ➢ Có thể tái tạo nhưng chỉ với một khoảng thời gian và tình huống cụ thể
  - ➢ Dễ tái tạo mọi lúc mọi nơi

❸ Phân tích RR theo mức độ

Xác Suất xảy ra:

- Khả năng khai thác_ E: mức độ khó sử dụng lỗ hổng để thực hiện cuộc tấn công? Khả năng khai thác được mô tả thành bốn cấp độ:

➢ Expert nghĩa là việc khai thác chưa được công bố, khó thực hiện và yêu cầu kiến thức nội bộ đáng kể và chuyên môn kỹ thuật hoặc nhiều lỗ hổng phải được khai thác trước khi có thể nhận ra bất kỳ tác động nào.

➢ ourneyman có nghĩa là khai thác chưa được công bố, khó thực hiện và yêu cầu kiến thức nội bộ hoặc chuyên môn kỹ thuật đáng kể.

➢ Adept có nghĩa là việc khai thác được biết đến bao gồm thông tin kỹ thuật và / hoặc nội bộ nhưng khó thực hiện và không có sẵn mã khai thác.

➢ Novice có nghĩa là việc khai thác đã được biết đến nhiều và tập lệnh tự động đã được cung cấp để những đứa trẻ tập lệnh có thể chạy để khai thác lỗ hổng.

❸ Phân tích RR theo mức độ

Xác Suất xảy ra:

Khả năng phát hiện (Discoverability_ D2)

Khả năng khám phá đề cập đến mức độ khó tìm thấy?

- Khó có nghĩa là lỗ hổng bảo mật bị che khuất và người dùng khó có thể tìm ra thiệt hại tiềm năng.
- Trung bình có nghĩa là lỗ hổng bảo mật nằm ở một phần sản phẩm hiếm khi được sử dụng và chỉ một số người dùng mới bắt gặp. Sẽ mất một số suy nghĩ để thấy việc sử dụng độc hại ..
- Dễ dàng có nghĩa là thông tin được công bố giải thích cuộc tấn công. Lỗ hổng được tìm thấy trong các tính năng thường được sử dụng và rất đáng chú ý.

2. Phân tích rủi ro (Risk Analysis)

❹ Phương pháp định lượng phân tích rủi ro RE theo phương pháp DREAD

Mức độ rủi ro: RE = (D + R + E + A + D2)/5

Mỗi danh mục được đưa ra một xếp hạng, ví dụ: 3 cao, 2 cho trung bình, 1 cho thấp và 0 cho không.

Thang đánh giá chạy từ 0 đến 10 là phổ biến. Phép tính luôn tạo ra một số từ 0 đến 10; số càng cao, rủi ro càng nghiêm trọng, trong đó 0 cho thấy không có tác động và 10 là kết quả tồi tệ nhất có thể xảy ra.

Nếu điểm của DREAD trên 7 điểm, rủi ro đó rất quan trọng

2. Phân tích rủi ro (Risk Analysis)

Một số câu hỏi gợi ý trong quá trình phân tích rủi ro

Mức độ thiệt hại như thế nào?

Xác suất xảy ra cao hay thấp?

Mức độ rủi ro có thể chấp nhận?

Rủi ro được xử lí như thế nào?

Nguyên nhân của rủi ro?

Có điểm tương đồng giữa các rủi ro?

Có phụ thuộc vào mối quan hệ?

Những yếu tố của rủi ro?

3

Đánh giá đe dọa của rủi ro

3. Đánh giá đe dọa của rủi ro

Tầm quan trọng của đánh giá rủi ro

- Đánh giá rủi ro là một hoạt động khá cần thiết và quan trọng

Mục tiêu và nội dung đánh giá rủi ro

- ✓ Đánh giá rủi ro tập trung vào việc xác định hoặc đo lường mức độ tổn thất và khả năng (hoặc xác suất) xảy ra của các nguy cơ rủi ro được nhận diện.
- ✓ Sắp xếp thứ tự ưu tiên các loại rủi ro cần quản trị

3. Đánh giá đe dọa của rủi ro

Các lưu ý trong đánh giá rủi ro

- ✓ Đánh giá rủi ro đòi hỏi kiến thức sâu rộng về các hoạt động trong doanh nghiệp, thị trường và môi trường kinh doanh
- ✓ Doanh nghiệp phải thiết lập các tiêu chí đánh giá rủi ro
- ✓ Một nguyên nhân có thể gây ra nhiều loại tổn thất khác nhau hoặc nhiều nguyên nhân, nhiều mối nguy có thể dẫn đến một loại tổn thất

3. Đánh giá đe dọa của rủi ro

Các đại lượng đánh giá rủi ro

* 2 đại lượng cơ bản:

- Tần suất xảy ra rủi ro (frequency/probability): khả năng hay số lần rủi ro có thể xảy ra trong một thời gian nhất định (thường là một năm)
- Mức độ nghiêm trọng hay độ lớn của các rủi ro/ tổn thất có thể xảy ra (severity)

Các phương pháp đánh giá

Phương pháp định lượng

Đánh giá định lượng ước tính được tần suất xảy ra và mức độ nghiêm trọng của tổn thất theo các đơn vị tính cụ thể.

- Yêu cầu một cơ sở dữ liệu đủ lớn
- Phù hợp cho các rủi ro đã từng xảy ra tổn thất
- Không tính đến sự thay đổi của môi trường kinh doanh
- Khó triển khai trong thực tế

Các phương pháp đánh giá

Phương pháp đánh giá định tính

- Đánh giá định tính xác định tần suất xảy ra, mức độ nghiêm trọng hoặc mức rủi ro chung theo các tiêu chí định tính
- Sử dụng cách chấm điểm cho từng tiêu chí dựa trên kinh nghiệm và đánh giá của người chấm
- Áp dụng đối với các rủi ro khó đo lường định lượng, khi môi trường kinh doanh có sự biến động

3. Đánh giá đe dọa của rủi ro

Tần suất/ khả năng xảy ra

Ví dụ 1: Rủi ro bị tấn công bởi virus

- Hiếm khi xảy ra: có thể xảy ra sau 1 năm
- Khó xảy ra: có thể xảy ra trong thời gian 6 tháng đến 1 năm
- Có thể xảy ra: có thể xảy ra trong thời gian 6 tháng
- Dễ xảy ra: có thể xảy ra 1 lần/ tháng
- Hầu như chắc chắn xảy ra: có thể xảy ra nhiều lần trong 1 tháng

3. Đánh giá đe dọa của rủi ro

Tần suất/ khả năng xảy ra

Ví dụ 2: Đánh giá rủi ro trong bị “bom” hàng

- Luôn luôn xảy ra: 5 điểm
- Rất thường xảy ra: 4 điểm
- Thường xảy ra: 3 điểm
- Hiếm khi xảy ra: 2 điểm
- Hầu như không xảy ra: 1 điểm

Các phương pháp đánh giá

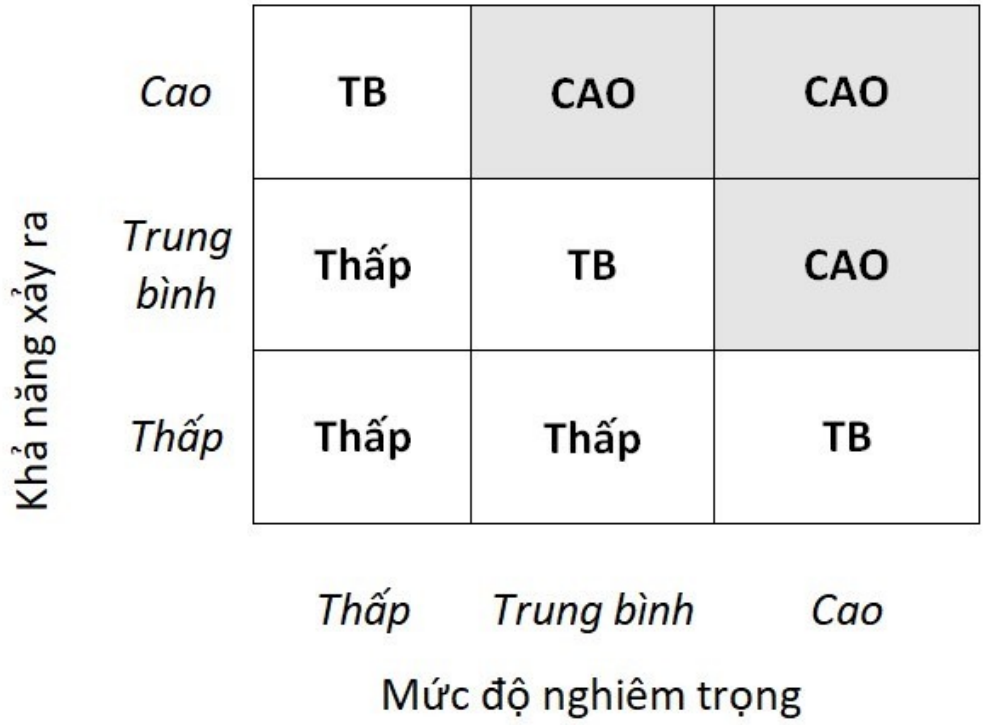
Phương pháp sử dụng các quy trình (lưu đồ)

- Nội dung của phương pháp
- Ưu điểm: có thể nhận dạng nhiều loại rủi ro (nhất là các rủi ro hoạt động, rủi ro vận hành, rủi ro trong sản xuất)
- Hạn chế: không sử dụng được nếu doanh nghiệp không có các quy trình công việc

Ma trận đo lường rủi ro

Tần suất xuất hiện Mức độ nghiêm trọng	Cao	Thấp
Cao	I	II
Thấp	III	IV

Ma trận đo lường rủi ro



CHƯƠNG 4

Giải pháp về pháp lý đối phó với rủi ro trong thương mại điện tử

NỘI DUNG

1. Khái niệm và chiến lược kiểm soát rủi ro
2. Quy trình kiểm soát rủi ro
3. Các giải pháp kiểm soát rủi ro trong TMĐT
4. Biện pháp bảo vệ trong thương mại điện tử

1

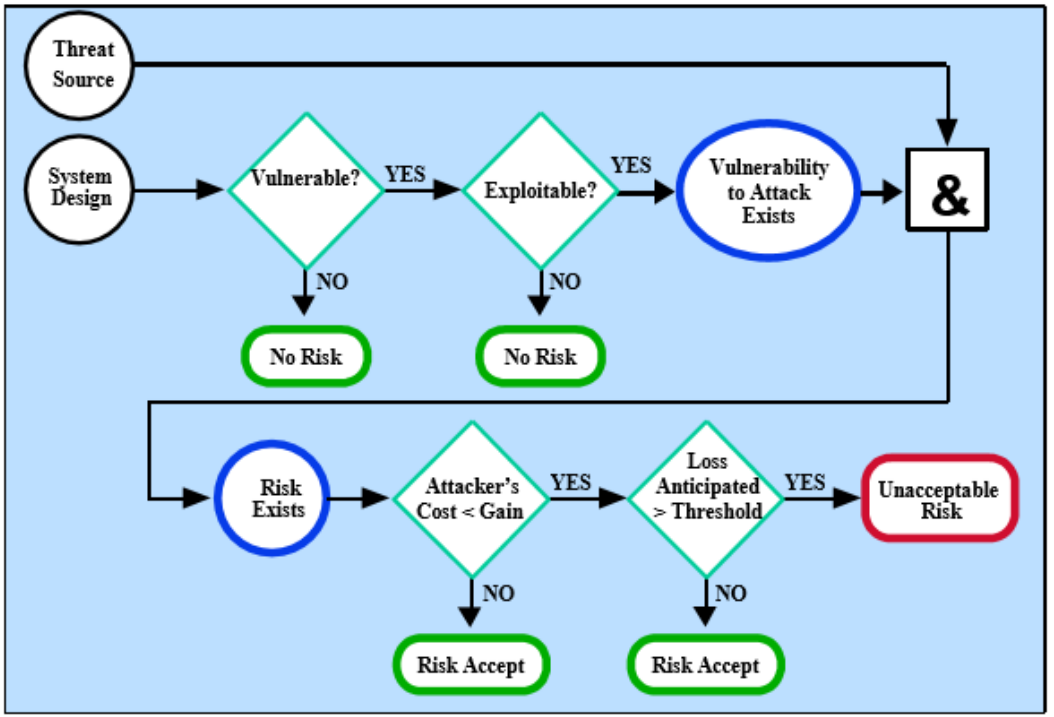
Khái niệm và chiến lược kiểm soát rủi ro

1. Kiểm soát rủi ro TMĐT

- **Kiểm soát rủi ro** là quá trình thực hiện các biện pháp để ngăn chặn hoặc giảm thiểu rủi ro có thể xảy ra đối với một công việc, hoạt động, quá trình hoặc tài sản.
- Quá trình kiểm soát RR được thực hiện theo phân cấp quản lý và tuân thủ các quy trình kỹ thuật. Điều quan trọng là quá trình kiểm soát rủi ro không tạo ra những mối nguy hiểm mới, và hiệu quả của các kiểm soát được theo dõi liên tục.

1. Kiểm soát rủi ro TMĐT

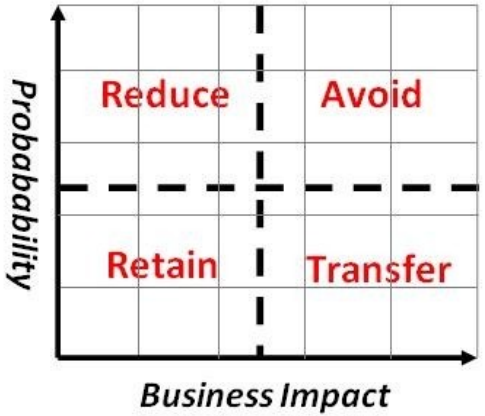
Kiểm soát rủi ro bắt đầu với việc chọn lựa chiến lược và phương pháp đối phó rủi ro. Có nhiều chiến lược và phương pháp đối phó khác nhau, tùy theo từng tình huống, môi trường và đặc thù của từng rủi ro.



1. Kiểm soát rủi ro TMĐT

Các chiến lược kiểm soát rủi ro

1. Tránh rủi ro ➔ Khi tồn tại lỗ hổng
2. Giảm nhẹ rủi ro ➔ Khi một lỗ hổng có thể được thực hiện
3. Chuyển giao ➔ Khi chi phí của kẻ tấn công là nhỏ hơn so với lợi ích có được
4. Chấp nhận rủi ro ➔ Khi tổn thất là quá lớn



Các chiến lược kiểm soát rủi ro

Tránh rủi ro (Risk Avoidance): Tránh rủi ro là kỹ thuật QTRR đề cập đến:

- Tiến hành các bước để loại bỏ một nguy hiểm
- Lựa chọn hoạt động thay thế

Các chiến lược kiểm soát rủi ro

Giảm nhẹ rủi ro (Risk reduction): là một PP kiểm soát RR có sử dụng các kỹ thuật thích hợp để giảm bớt khả năng xảy ra một sự cố, một hậu quả hoặc cả hai...

Thực thi các biện pháp để giảm thiểu khả năng xảy ra RR hoặc giảm thiểu tác động và chi phí khắc phục RR nếu nó xảy ra.

Các chiến lược kiểm soát rủi ro

Chuyển giao RR (Risk transfer) là một biện pháp của kiểm soát rủi ro, được sử dụng trong quản trị RR để mô tả sự chuyển dịch của gánh nặng RR cho một bên khác.

Chuyển giao RR bằng cách chia sẻ tổn thất, thiệt hại khi chúng xảy ra.

Ví dụ: mua bảo hiểm tài sản

Ví dụ mua bảo hiểm tài sản

DỊCH VỤ BẢO HIỂM MÁY TÍNH Á ĐÔNG

I. Nội dung

Gói 1: Thực hiện việc bảo hiểm tại trung tâm bảo hiểm Á Đông

- Số lần sửa chữa miễn phí **không giới hạn** tại trung tâm

Gói 2: Thực hiện tận nơi khách hàng

- Số lần **sửa chữa miễn phí lên đến 24 lần** tận nơi khách hàng.

Gói 3: Thực hiện tận nơi khách hàng

- Số lần sửa chữa miễn phí **không giới hạn** tận nơi khách hàng.

Sàn giao dịch TMĐT
ĐÃ ĐĂNG KÝ
với Bộ Công Thương

I. Bảng giá *(Áp dụng từ ngày 01/06/2010)*

Dịch vụ bảo hiểm	Gói 1	Gói 2	Gói 3
Dành cho PC	365.000	420.000	730.000
Dành cho Laptop	395.000	520.000	790.000

Trusted Choice®

* Thẻ Bảo hiểm có giá trị cho 1 đơn vị thiết bị (máy tính, thiết bị ngoại vi)/12 tháng

Các chiến lược kiểm soát rủi ro

- **Chấp nhận rủi ro (Risk Acceptance)** được sử dụng trong quản trị RR để mô tả một quyết định chấp nhận những hậu quả và khả năng của một RR cụ thể.
- Chấp nhận RR hoặc "sống chung" với RR trong trường hợp chi phí loại bỏ, phòng tránh, làm nhẹ RR quá lớn (lớn hơn chi phí khắc phục tác hại), hoặc tác hại của RR nếu xảy ra là nhỏ hay cực kỳ thấp.
- Việc lựa chọn PP kiểm soát RR nào phụ thuộc vào nhiều yếu tố. Đối với DN, lựa chọn PP kiểm soát RR có thể xem là một chiến lược đối phó hợp lý.
- Hoạt động giám sát RR cũng được thực hiện để bảo đảm các chiến lược đối phó rủi ro được đúng kế hoạch và thực thi chặt chẽ.

2

Quy trình kiểm soát rủi ro

Các mục tiêu của kiểm soát rủi ro

Mục tiêu trước khi tổn thất xảy ra

- ✓ Chuẩn bị để đối phó với rủi ro tiềm ẩn một cách tiết kiệm nhất.
- ✓ Giảm thiểu sự lo lắng của các cấp lãnh đạo và các nhà quản lý doanh nghiệp
- ✓ Đáp ứng các yêu cầu và quy định của pháp luật.

Các mục tiêu của kiểm soát rủi ro

Mục tiêu sau khi tổn thất xảy ra

- ✓ Bảo đảm sự tồn tại sống còn của doanh nghiệp
- ✓ Tiếp tục hoạt động và tăng trưởng
- ✓ Bảo đảm sự ổn định doanh thu
- ✓ Hạn chế sự suy giảm của lợi nhuận
- ✓ Làm giảm các tác động tiêu cực của tổn thất do rủi ro gây ra lên xã hội và con người

Quy trình kiểm soát rủi ro

Nhận diện và đánh giá rủi ro

* Các câu hỏi định hướng:

+ Doanh nghiệp đang phải đối mặt với những rủi ro nào?

+ Các rủi ro có khả năng xảy ra và mức độ nghiêm trọng như thế nào?

+ Có những rủi ro nào cần phải lưu ý và cần ưu tiên quản trị ?

Quy trình kiểm soát rủi ro

Nghiên cứu tính khả thi của các phương pháp kiểm soát rủi ro

* Các câu hỏi định hướng:

+ Các phương pháp kiểm soát rủi ro là gì ?

+ Các phương pháp tài trợ rủi ro là gì?

+ Ưu điểm và hạn chế của từng phương pháp?

….

Quy trình kiểm soát rủi ro

Lựa chọn phương pháp quản trị rủi ro tối ưu

Các cơ sở để lựa chọn:

- Về mặt tài chính
- Các yếu tố phi tài chính

Quy trình kiểm soát rủi ro

Triển khai chương trình quản trị rủi ro

* Các công cụ hỗ trợ:

- ***Tuyên bố về chính sách quản trị rủi ro:*** mục tiêu, quan điểm cơ bản về quản trị rủi ro của doanh nghiệp
- ***Sổ tay quy trình quản trị rủi ro:*** nguyên tắc chỉ đạo, quy trình thực hiện, trách nhiệm và quyền hạn
- ***Hệ thống thông tin quản trị rủi ro***

Quy trình kiểm soát rủi ro

Giám sát, đánh giá hiệu quả quản trị rủi ro

* Các câu hỏi định hướng:

+ Mục tiêu nào đã đạt được? Mục tiêu nào chưa đạt ?

+ Những sai sót nào xảy ra trong quá trình thực hiện?

+ Chương trình phòng chống tổn thất có hiệu quả không?

+ Chương trình quản trị rủi ro cũ có cần điều chỉnh gì?

3

Các giải pháp kiểm soát rủi ro trong thương mại điện tử

Các giải pháp đối phó rủi ro trong thương mại điện tử

Giải pháp đối phó là một hành động, thiết bị, thủ tục, hoặc kỹ thuật làm giảm mối đe dọa, một lỗ hổng, hoặc một cuộc tấn công bằng cách loại bỏ hoặc ngăn chặn nó, bằng cách giảm thiểu các tác hại nó có thể gây ra, hoặc bằng cách phát hiện và thông báo để sửa chữa, khắc phục các hành động có thể được thực hiện.

Phân loại giải pháp kiểm soát rủi ro

Theo các biện pháp đối phó

Theo thời gian

Theo đối tượng

Theo quản lý và vận hành

Phân loại giải pháp đối phó

- Chính sách an toàn (security policy)
- An toàn thông tin của tổ chức
- Quản trị tài sản
- An toàn nguồn nhân lực
- An toàn vật lý và môi trường
- Quản trị vận hành và truyền thông

- Phần mềm chống Virus
- Phần mềm Anti keyloggers
- Live CD/USB
- Giám sát, theo dõi mạng
- Automatic form filler programs
- One-time passwords (OTP)
- Security tokens

Phân loại giải pháp đối phó

- Kiểm soát truy cập
- Tiếp nhận, bảo trì và phát triển các hệ thống thông tin
- Quản trị sự cố an toàn thông tin
- Quản trị kinh doanh liên tục
- Tuân thủ pháp luật và nội quy
- On-screen keyboards
- Phần mềm can thiệp
- Nhận biết giọng Nhận biết vân tay và cử chỉ nhấp chuột
- Thu âm
- Biện pháp phi kỹ thuật

Ví dụ đối phó với Phishing

Ảnh hưởng, tác hại:

- Lừa dối tiết lộ thông tin
- Cho phép kẻ thù truy cập vào thông tin cá nhân, tổ chức

Biện pháp đối phó:

- ✓ Cảnh giác
- ✓ Xóa bỏ thư điện tử khả nghi
- ✓ Contact your system security point of contact with any questions
- ✓ Báo cáo bất cứ nguy cơ tiềm ẩn nào
- ✓ Tìm kiếm chữ kí số
- ✓ Sử dụng IDS để chặn, khóa các địa chỉ IP, tên miền
- ✓ Cài đặt và cập nhật phần mềm chống vi rút.

Phân loại giải pháp kiểm soát rủi ro

Theo các biện pháp đối phó

Theo thời gian

Theo đối tượng

Theo quản lý và vận hành

Phân loại giải pháp kiểm soát rủi ro

Phân loại kiểm soát RR - theo thời gian

- ***Kiểm soát phòng ngừa (preventive controls):*** Trước sự cố xảy ra, nhằm ngăn chặn một sự cố xảy ra
- ***Kiểm soát phát hiện (detective controls):*** cùng với sự cố xảy ra, nhằm phát hiện và mô tả một sự cố trong quá trình
- ***Kiểm soát điều chỉnh (corrective controls):*** sau sự cố, nhằm hạn chế mức độ thiệt hại gây ra bởi sự cố
- Khác: kiểm soát ngăn chặn (deterrent controls), kiểm soát bồi thường (compensation)

Phân loại giải pháp kiểm soát rủi ro

Phân loại kiểm soát RR - theo đối tượng, có 4 loại

- Kiểm soát vật lí (Physical controls)
- Kiểm soát thủ tục (Procedural controls)
- Kiểm soát kỹ thuật (Technical controls)
- Kiểm soát tuân thủ quy định (Legal and regulatory or compliance controls)

Phân loại kiểm soát RR - theo quản lý và vận hành, 03 loại

- Kiểm soát kỹ thuật (Technical Security Controls)
- Kiểm soát quản trị (Management Security Controls)
- Kiểm soát vận hành (Operational Security Controls)

Phân loại kiểm soát RR - theo quản lý và vận hành

❶ Kiểm soát kỹ thuật

Bao gồm 3 loại: Kiểm soát kỹ thuật hỗ trợ; Kiểm soát kỹ thuật ngăn ngừa; và Kiểm soát kỹ thuật phát hiện và phục hồi

1. Kiểm soát kỹ thuật hỗ trợ:

- Nhận biết Identification
- Quản lý Khóa mật mã (Cryptographic Key Management
- Quản lý an ninh (Security Administration)
- Bảo vệ hệ thống (System Protections)

Phân loại kiểm soát RR - theo quản lý và vận hành

❶ Kiểm soát kỹ thuật

2. Kiểm soát kỹ thuật ngăn ngừa

- Xác thực (Authentication)
- Ủy quyền (Authorization):
- Thực thi kiểm soát truy cập (Access Control Enforcement)
- Chống chối bỏ (Nonrepudiation)
- Kiểm soát truyền thông được bảo vệ (Protected Communications)
- Giao dịch bí mật (Transaction Privacy)

Phân loại kiểm soát RR - theo quản lý và vận hành

❷ Kiểm soát vận hành

1. Kiểm soát vận hành ngăn ngừa:

- Cung cấp khả năng sao lưu
- Bảo vệ laptops, PC, máy chủ
- Cung cấp nguồn điện dự phòng
- Thiết lập các thủ tục lưu trữ off-site và an toàn
- Bảo vệ tài sản IT từ cháy, nổ, các sự cố môi trường
- Kiểm soát độ ẩm và nhiệt độ thiết bị

2. Kiểm soát vận hành phát hiện

- Cung cấp bảo đảm an toàn vật lý
- Bảo đảm an toàn môi trường

Các hệ thống phát hiện xâm nhập IDS

• **Hệ thống phát hiện xâm nhập (IDS):** là một thiết bị hoặc phần mềm ứng dụng giám sát hệ thống hoặc hoạt động mạng nhằm phát hiện hiện tượng bất thường, các hoạt động trái xâm nhập phép và hệ thống. IDS có thể phân biệt được những tấn công từ bên trong hay từ bên ngoài.

• IDS phát hiện dựa trên các dấu hiệu đặc biệt về các nguy cơ đã biết hay dựa trên so sánh lưu thông mạng hiện tại với thông số đo đạt chuẩn của hệ thống (baseline) để tìm ra các dấu hiệu khác thường.

Các biện pháp xử lý rủi ro khác

- **Các biện pháp phi công nghệ**
  - Đòn bẩy rủi ro
  - Sử dụng biểu đồ GANTT trong kiểm soát RR
  - Cây quyết định

Các biện pháp công nghệ

Đòn bẩy rủi ro

• Đòn bẩy rủi ro (Risk leverage) là công cụ sử dụng để so sánh biện pháp đối phó RR nào hiệu quả. Đòn bẩy rủi ro/đòn bẩy giảm rủi ro (Risk Reduction Leverage) là một phương pháp đơn giản đưa ra một giá trị với một biện pháp đối phó, có thể các biện pháp đối phó khác nhau để so sánh.

• RL (RRL) được xác định: RL = Sự thay đổi trong mức độ rủi ro/ Chi phí để thực hiện một biện pháp đối phó

• RL = (Mức độ rủi ro trước khi giảm bớt – Mức độ rủi ro sau khi giảm bớt)/Chi phí của giảm rủi ro.

PP định lượng phân tích rủi ro
RE

Mức độ rủi ro (RE) là rủi ro được xác định dựa trên giá trị tài sản tổn thất L(o) và khả năng xảy ra tổn thất P(o). Khi đó: Mức độ rủi ro:

$$RE = P(O) \times L(O)$$

RL (RRL) được xác định: RL = Sự thay đổi trong mức độ rủi ro/ Chi phí để thực hiện một biện pháp đối phó

RL = (Mức độ rủi ro trước khi giảm bớt – Mức độ rủi ro sau khi giảm bớt)/Chi phí của giảm rủi ro.

Ví dụ

• Ví dụ 1: Mức độ RR trước đối phó là: 5000K; Mức độ RR sau khi can thiệp: 3000K; Chi phí can thiệp RR: 1500K

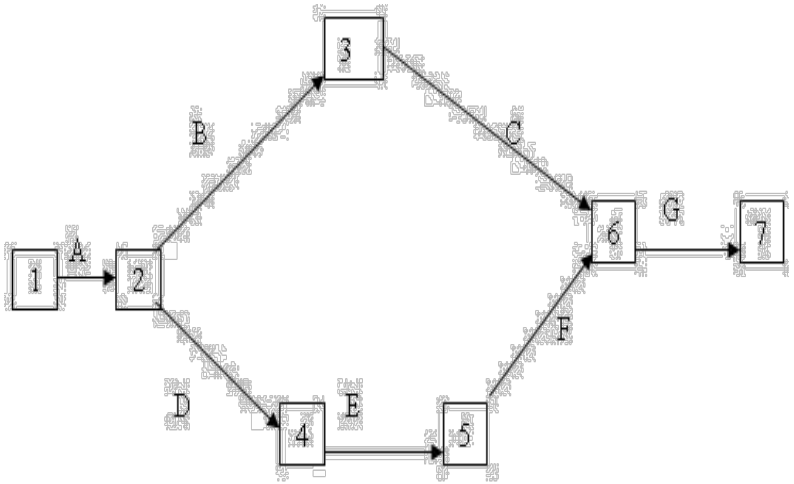
➔ RRL = (5000K – 3000K)/1500K = 1,33 > 1

• Câu hỏi: Có sử dụng biện pháp can thiệp hay không?

• Trả lời: Đáng làm

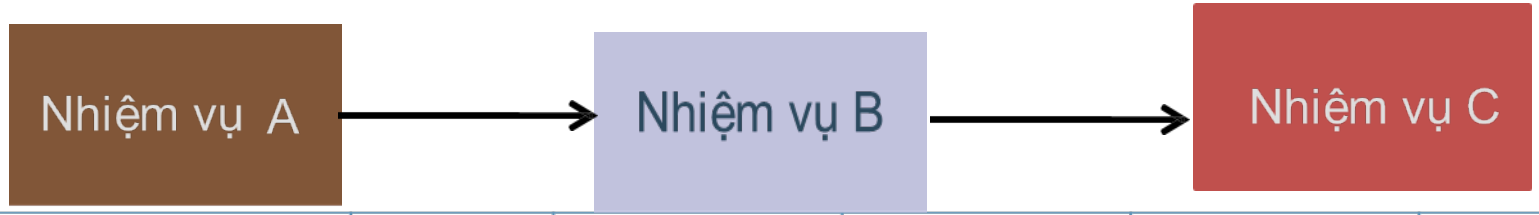
Kỹ thuật kiểm tra và đánh giá việc thực hiện

Viết tắt là **PERT (Performance Evaluation and Review Technique)** được phát minh ra năm 1958 khi phát triển tên lửa Polaris . Ban đầu PERT chỉ được dùng để mô tả một dãy các hoạt động qua một tập các mũi tên. Mỗi mũi tên biểu thị cho một hoạt động và được gắn nhãn theo tên hoạt động đó, chẳng hạn A, B, C…



Sử dụng GANTT trong kiểm soát RR

- Ví dụ: một dự án với ba nhiệm vụ thực hiện



Nhiệm vụ	a	m	b	t_e	S
A	10	12	16	?	?
B	8	10	14	?	?
C	20	24	38	?	?

- Thời gian kì vọng hoàn thành dự án: 12.33 + 10.33 + 25.66 = 48.32
- Sai số chuẩn (độ lệch chuẩn) cho chuỗi nhiệm vụ A + B+ C là:

$$\sqrt{(1^2 + 1^2 + 3^2)} = 3.32$$

Bài toán 1

Hãy vẽ sơ đồ PERT cho kế hoạch sau, tô đậm đường Gantt. Chiều dài dự án là bao nhiêu?

Hoạt động	Thời hạn (ngày)	Hoạt động trước
A	3	-
B	5	A
C	3	A
D	11	B
E	7	B
F	4	C
G	9	E, F
H	2	D, G

1.1.4. Các chi phí rủi ro (Cost of risk)

4 thành phần:

Chi phí tổn thất ước tính: phát sinh trực tiếp

& gián tiếp từ hậu quả bất lợi của rủi ro

Chi phí kiểm soát rủi ro: chi phí ngăn ngừa, khắc phục, hạn chế tổn thất

Chi phí tài trợ tổn thất: phí bảo hiểm

Chi phí hành chính liên quan đến các chương trình QTRR

4

Biện pháp bảo vệ trong thương mại điện tử

Biện pháp bảo vệ trong thương mại điện tử

- Bảo vệ cá nhân
- Bảo vệ doanh nghiệp
- Lưu ý khi giao dịch thương mại điện tử

Biện pháp bảo vệ trong thương mại điện tử

4.1. Bảo vệ cá nhân

- Khi nhận spam → xóa bỏ hết
- Không click vào bất kỳ đường link nào trong email
- Không mở lên các file gửi kèm trong email.
- Đừng trả lời những email spam
- Ngay cả chức năng “Từ chối nhận” (Unsubscription) cũng đã bị lợi dụng để người gửi spam kiểm tra tính hiện hữu của tài khoản email,
- Cài những chương trình chống virus mới nhất, cập nhật chương trình thường xuyên.

4.1. Bảo vệ cá nhân

- Bỏ qua mọi email yêu cầu cung cấp thông tin cá nhân. Hầu hết tất cả đó đều là trò lừa đảo hoặc có âm mưu gián điệp (spyware) hay virus. Ngân hàng hay dịch vụ thanh toán qua mạng không bao giờ yêu cầu thông tin “nhạy cảm” qua mạng Internet. Nếu có yêu cầu thì đó phải là form nhập thông tin từ website của chính tổ chức đó, với giao thức truyền an toàn (https://)
- Nếu cá nhân có thẻ tín dụng và có mua qua mạng thì phải kiểm tra kỹ từng khoản chi tiêu mỗi tháng được liệt kê trong hóa đơn ngân hàng gửi về để kịp thời phát hiện sự cố nếu có.

4.1. Bảo vệ cá nhân

- Khi nhận được những email từ người lạ với những file gửi kèm thì phải rất cẩn thận.
- Trong khi lướt web nếu thấy xuất hiện những thông báo đề nghị cài đặt hay thông báo nào khác thì nên đọc kỹ, không dễ dàng chọn “OK” hay “Yes”.
- Sau khi truy cập vào tài khoản email hay tài khoản quan trọng nào khác thì nhớ Log-off để thoát hoàn toàn ra khỏi trang web, tránh người khác dùng máy tính đó trong vài phút sau có thể truy cập vào được.
- Nếu phải dùng máy tính dùng chung thì không nên dùng chức năng “Nhớ Password”.

4.1. Bảo vệ cá nhân

- Sử dụng chương trình bản quyền
- Sử dụng trình diệt virus
- Sử dụng tường lửa

Biện pháp bảo vệ trong thương mại điện tử

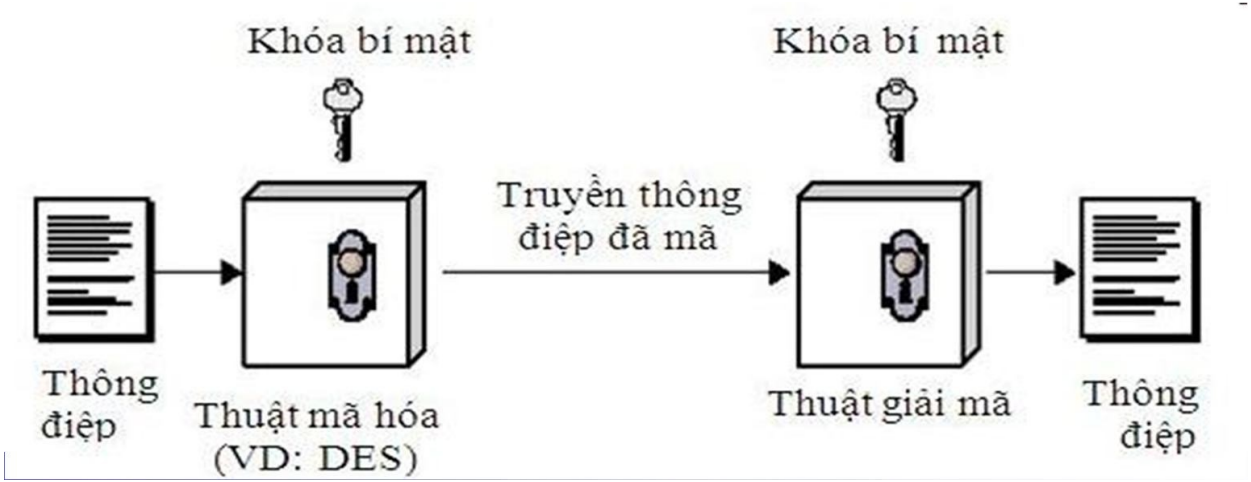
4.2. Bảo vệ phía doanh nghiệp

- Bảo mật trong giao dịch
- Kiểm tra tính đúng đắn và chân thực của thông tin trong giao dịch
- Lưu trữ dữ liệu nhiều nơi với nhiều hình thức
- Cài đặt các phần mềm chống Virút tấn công
- Tham gia bảo hiểm


4.2.1. Bảo mật trong giao dịch
Mã hóa dữ liệu
Mã hóa khóa bí mật
Mã hóa khóa công cộng
Chữ ký số
Phong bì số
Cơ quan chứng thực
Ứng dụng PKI

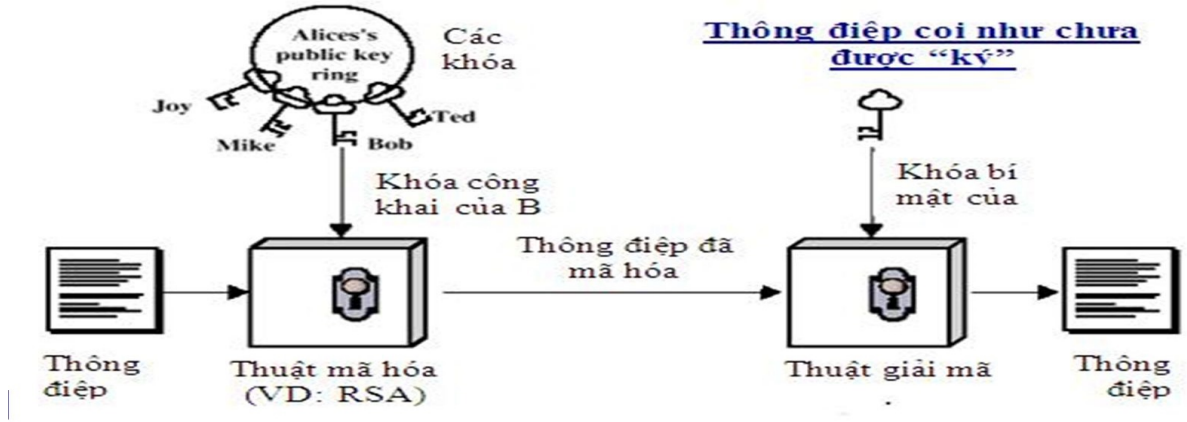
Mã hoá khoá bí mật

Mã hoá khoá bí mật (Secret key Crytography): Mã hoá khoá bí mật hay còn gọi là mã hoá đối xứng, nghĩa là dùng một khoá cho cả hai quá trình “mã hóa” và “giải mã”. Khóa này phải được giữ bí mật.



Mã hoá công khai

Mã hoá công khai (Public key Crytography): Mã hoá công khai hay còn gọi là mã hoá không đối xứng. Phương pháp này người ta sử dụng hai khoá khác nhau, khoá công khai (public key) và khóa bí mật (Private key). Khóa công khai được công bố, khóa bí mật được giữ kín.



Chữ ký số (digital signature)

- Sử dụng chữ ký điện tử nhằm đảm bảo tính toàn vẹn, duy nhất và không bị sửa đổi bởi người khác của dữ liệu trong giao dịch.

- Chữ ký điện tử là một công cụ bảo mật an toàn nhất hiện nay. Nó là bằng chứng xác thực người gửi chính là tác giả của thông điệp mà không phải là một ai khác

- Chữ ký điện tử được gắn với một thông điệp điện tử thì đảm bảo rằng thông tin trên đường chuyển đi sẽ không bị thay đổi bởi bất kỳ một người nào ngoài người ký ban đầu. Mọi sự thay đổi dù nhỏ nhất sẽ đều bị phát hiện một cách dễ dàng.

- Chữ ký điện tử có thể là chữ ký tự đánh từ bàn phím, một bản quét của chữ viết tay; một âm thanh, biểu tượng; một thông điệp được mã hoá hay dấu vân tay, giọng nói...

Phong bì số (Digital Envelope)

- Tạo lập một phong bì số là một quá trình mã hoá một chìa khoá bí mật (chìa khoá DES) bằng khoá công khai của người nhận.
- Chìa khoá bí mật này được dùng để mã hoá toàn bộ thông tin mà người gửi muốn gửi cho người nhận và phải được chuyển cho người nhận để người nhận dung giải mã những thông tin.

Cơ quan chứng thực (Certificate Authority – CA)

- Cơ quan chứng thực là một tổ chức nhà nước hoặc tư nhân đóng vai trò là người thứ 3 đáng tin cậy trong thương mại điện tử để xác định nhân thân của người sử dụng khoá công khai.

- Sự xác nhận của CA về chữ ký điện tử, về lai lịch của người ký, thông điệp của người ký và tính toàn vẹn của nó là rất quan trọng trong giao dịch điện tử.

- Cơ quan chứng thực có vai trò quan trọng, bởi trong thương mại điện tử, các bên tham gia không gặp mặt trực tiếp nhau và đôi khi không quen biết nhau nên rất cần có sự đảm bảo của người thứ 3.

- Hệ thống bảo mật hiện nay đảm bảo độ an toàn rất cao, gần như là tuyệt đối, song việc thực hiện phụ thuộc vào trình độ cũng như thực trạng cơ sở hạ tầng tin học của các bên.

4.2. Bảo vệ phía doanh nghiệp

4.2.2. Kiểm tra tính đúng đắn và chân thực của thông tin trong giao dịch

Mặc dù đã sử dụng những biện pháp kỹ thuật để bảo mật thông tin, song khi nhận được các thông tin người sử dụng vẫn phải kiểm tra tính đúng đắn, chân thật của thông tin.

Giao dịch trên mạng là loại hình giao dịch không biên giới có tính chất toàn cầu. Các bên giao dịch không gặp nhau, thậm chí không hề quen biết nhau, và đây cũng chính là cơ hội để cho kẻ xấu lợi dụng để thực hiện mục đích của mình.

Vì vậy, việc kiểm tra tính đúng đắn và chân thật của thông tin trong giao dịch cần phải được thực hiện thường xuyên để phòng tránh những rủi ro như thông tin gây nhiễu, giả mạo hay lừa đảo. Các biện pháp kiểm tra cần tuỳ theo tình huống cụ thể mà áp dụng. Có thể dùng các phương pháp kỹ thuật hoặc phương pháp điều tra mang tính xã hội...

4.2. Bảo vệ phía doanh nghiệp

4.2.3. An toàn mạng (Network security)

- An toàn mạng bao gồm các chính sách và thực tế áp dụng để ngăn chặn và giám sát truy cập trái phép, sử dụng sai, sửa đổi, hoặc từ chối của một mạng máy tính và các tài nguyên mạng có thể truy cập.
- An toàn mạng đề cập đến việc cấp phép truy cập vào dữ liệu trong một mạng (được kiểm soát bởi quản trị mạng). Người sử dụng chọn hoặc được chỉ định một ID và mật khẩu hoặc các thông tin chứng thực khác để truy cập thông tin và các chương trình theo thẩm quyền của mình.
- An toàn mạng bao gồm một loạt các mạng máy tính, cả công cộng và tư nhân, được sử dụng trong công việc hàng ngày; thực hiện giao dịch và truyền thông giữa các DN, CP, CN. An toàn mạng là bảo vệ mạng, là giám sát các hoạt động được thực hiện.

An toàn Internet (internet security)

- An toàn Internet là một nhánh của an toàn máy tính, liên quan đến Internet, thường đề cập đến an toàn trình duyệt (Browser security) cũng như an toàn dữ liệu nhập vào dưới dạng web, và xác thực tổng thể và bảo vệ dữ liệu gửi qua giao thức Internet.

- Internet là một kênh không an toàn cho việc trao đổi thông tin dẫn đến khả năng rủi ro bị xâm nhập, gian lận, lừa đảo cao. Mục tiêu của an toàn Internet là thiết lập các quy tắc và các biện pháp để chống lại các cuộc tấn công trên Internet

Phân biệt An toàn mạng và An toàn máy tính

An toàn mạng	An toàn máy tính
Biện pháp để bảo vệ mạng riêng. Là loại hình bảo vệ bao gồm bất kỳ máy tính nào kết nối vào mạng	thiết kế để bảo vệ một đơn vị duy nhất hoặc một máy tính
Đề cập đến việc đảm bảo sử dụng, tính toàn vẹn và an toàn mạng riêng và bất kỳ dữ liệu liên quan đến mạng	Mức độ bảo mật là tương tự và phòng ngừa nhiều vấn đề tương tự. Tuy nhiên, hầu hết các DN kết hợp cả an toàn máy tính và an toàn mạng để thiết lập mức độ bảo vệ cao nhất.

An toàn trình duyệt (Browser security)

Là ứng dụng an toàn Internet cho các trình duyệt web để bảo vệ dữ liệu mạng và các hệ thống máy tính từ vi phạm bí mật riêng tư hoặc phần mềm độc hại.

Khai thác an toàn trình duyệt cũng có thể lợi dụng các lỗ hổng bảo mật (security holes) và thường được sử dụng với tất cả các trình duyệt như Mozilla Firefox, Google Chrome, Opera, Microsoft Internet Explorer, và Safari.

An toàn di động (mobile security)

- An toàn di động (mobile security) hoặc an toàn điện thoại di động ngày càng quan trọng trong máy tính di động (mobile computing). Quan tâm đặc biệt là sự an toàn của thông tin cá nhân và kinh doanh hiện nay được lưu trữ trên điện thoại thông minh.

- Ngày càng có nhiều cá nhân và doanh nghiệp sử dụng điện thoại thông minh để quản trị, lưu trữ thông tin cá nhân, và công việc. Việc lưu trữ thông tin và kết nối Internet là nguồn gốc của những RR mới cho người dùng.

4.2. Bảo vệ phía doanh nghiệp

4.2.4. Bảo vệ các hệ thống của khách hàng và máy phục vụ

Các đe dọa đối với máy khách

- Các chương trình gây hại được phát tán thông qua các trang web, có thể phát hiện ra số thẻ tín dụng, tên người dùng và mật khẩu. Những thông tin này thường được lưu giữ trong các tệp đặc biệt – gọi là cookie. Các cookie được sử dụng để nhớ các thông tin yêu cầu của khách hàng, hoặc tên người dùng và mật khẩu. Nhiều nội dung động gây hại có thể lan truyền thông qua các cookie, chúng có thể phát hiện được nội dung của các tệp phía máy khách, hoặc thậm chí có thể hủy bỏ các tệp được lưu giữ trong các máy khách.

- Ví dụ, một virus máy tính đã phát hiện được danh sách các địa chỉ thư tín điện tử của người sử dụng và gửi danh sách này cho những người khác trên Internet

4.2. Bảo vệ phía doanh nghiệp

4.2.4. Bảo vệ các hệ thống của khách hàng và máy phục vụ

Các phương pháp phòng tránh

- ✓ Kiểm tra tính đúng đắn và chân thực của thông tin trong giao dịch
- ✓ Lưu trữ dữ liệu nhiều nơi với nhiều hình thức
- ✓ Cài đặt các phần mềm chống virut tấn công
- ✓ Tham gia bảo hiểm

5

Một vài lưu ý

Một vài đề nghị

Nếu là doanh nghiệp

- Thuê dịch vụ hosting (lưu trữ web), nhà cung cấp dịch vụ sẽ chịu trách nhiệm về việc tăng cường an toàn mạng, an toàn thông tin cho họ, và có nghĩa là cho cả website của ta.
- Sau khi login (đăng nhập) vào hệ thống quản lý website (do nhà cung cấp dịch vụ bàn giao lại cho bạn sử dụng), luôn phải thực hiện động tác logout (thoát) để đảm bảo các cửa ngõ phải được khóa lại ngay sau khi thoát ra.

Một vài đề nghị

Nếu là người mua

- Không truy cập vào hệ thống khi sử dụng máy tính công cộng; Không mở những email có file gửi kèm (attachment) mà người gửi có vẻ như xa lạ. Thậm chí đừng tin những email mang tên người gửi là Microsoft, Yahoo hay tương tự bởi vì đây có thể là thủ thuật giả danh của hacker để lừa .
- Về mối lo ngại bị ăn cắp số thẻ tín dụng khi mua hàng trên mạng và bán hàng cho người dùng thẻ tín dụng bất hợp pháp (thẻ bị ăn cắp).
  - ✓ Nếu là người mua: chỉ nên mua hàng ở những website tốt, tin cậy.
  - ✓ Làm sao để đánh giá website tin cậy ?

Một vài đề nghị

- Tên tuổi người bán
- Trình bày gian hàng một cách chuyên nghiệp, không có lỗi chính tả, câu cú rõ ràng v.v…
- Đọc phần About Us của họ để tìm một địa chỉ văn phòng cụ thể
- Đừng bao giờ cung cấp thông tin thẻ tín dụng cho các website khiêu dâm trên mạng.

Một vài đề nghị

Nếu là người bán :

- Nên nhờ trung gian để xử lý thẻ tín dụng
- Phải trả môt khoản chi phí % dựa trên doanh thu cho họ
- Đảm bảo kỹ thuật.
- Thông thường phải gửi hàng đi, khi người mua nhận được hàng →mới được nhận tiền vào tài khoản của bạn
- Nếu gặp phải thẻ tín dụng bất hợp pháp → sẽ mất trắng món hàng và mất một khoản chi phí xử lý thẻ
- Theo thống kê, chỉ có khoản 3% giao dịch là gặp phải trường hợp dùng thẻ tín dụng giả
- Khoản lời từ việc bán cho 97% khách hàng trung thực cũng đủ để bù cho khoản mất mát trong 3% gian lận này.

Chương 5

Nâng cao hiểu biết và ý thức của các chủ thể tham gia thương mại điện tử

NỘI DUNG

1. Chính sách sử dụng Internet
2. Chính sách sử dụng email
3. Bí mật riêng tư
4. Những nguyên tắc cơ bản về bảo vệ dữ liệu cá nhân trong TMĐT

1. Chính sách sử dụng Internet (IUP)

- Chính sách sử dụng Internet (IUP), chính sách sử dụng Internet được chấp nhận (IAUP) hoặc chính sách sử dụng Internet an toàn (ISP) hoặc (FUP) **Fair Use Policy** là một bộ quy tắc được áp dụng bởi nhà quản trị website, mạng máy tính hoặc các hệ thống thông tin trong đó hạn chế những cách thức mà các trang mạng hoặc hệ thống thông tin có thể được sử dụng.

1. Chính sách sử dụng Internet (IUP)

- IUP được viết cho các công ty, doanh nghiệp, trường học, nhà cung cấp dịchvụ truy cập Internet, chủ sở hữu website nhằm giảm rủi ro từcác hành động sử dụng mạng Internet của chính bởi các nhân viêntrong các tổ chức hoặc bất kì người sử dụng nào quan tâm.
- AUP là một phần của chính sách an ninh thông tin Internet security policies (ISP), quy định các thành viên của tổ chức tuân thủ khi truy cập/sử dụng Internet/các hệ thống thông tin

1. Chính sách sử dụng Internet (AUP)

- AUP phải súc tích, ngắn gọn và rõ ràng, bao gồm những điều quy định quan trọng về sử dụng (do), không được sử dụng (do not) đối với các trang mạng, hoặc các hệ thống thông tin của tổ chức.
- AUP cũng bao gồm những hướng dẫn sử dụng an toàn thông tin, quy định tuân thủ sử dụng an toàn thông tin.

1. Chính sách sử dụng Internet (AUP)

- AUP cũng cần có những quy định xử phạt khi người dùng không tuân theo quy định an toàn thông tin hoặc vi phạm quy định an toàn thông tin.

→ AUP/IAUP là một nội quy/điều lệ/văn bản tập hợp các hướng dẫn, các điều khoản, các quy định về điều kiện sử dụng Internet ở tổ chức, trường học và gia đình / hoặc khi sử dụng dịch vụ thông tin/ phương tiện điện tử tại các nơi công cộng.

1. Chính sách sử dụng Internet

- **Phân loại:**
  - **Chính sách an ninh thông tin**
    - Chính sách an ninh máy tính
    - Chính sách an ninh mạng máy tính

1. Chính sách sử dụng Internet

- **Phân loại:**
  - **Chính sách sử dụng Internet an toàn**
    - Chính sách sử dụng Internet được chấp nhận
    - Chính sách sử dụng e-mail được chấp nhận.
    - Chính sách đảm bảo bí mật thông tin cá nhân trên website
    - Chính sách đảm bảo bí mật thông tin cá nhân trên website B2C, cổng thanh toán điện tử

Internet Acceptable Use Policy

User Responsibilities

Rusk wig

These guidelines are intended to help you make the best use of the Internet resources at your disposal. You should understand the following.

1. The Organisation provides Internet access to staff to assist them in carrying out their duties for the Company. It is envisaged that it will be used to lookup details about suppliers, products, to access government information and other statutory information. It should not be used for personal reasons.

2. You may only access the Internet by using the Organisation's content scanning software, firewall and router.

3. You may only access the Internet after you have been authorised to do so by your department manager in writing.

When using the Organisation's Internet access facilities you should comply with the following guidelines.

DO

4. Do keep your use of the Internet to a minimum

5. Do check that any information you access on the Internet is accurate, complete and current.

6. Do check the validity of the information found.

7. Do respect the legal protections to data and software provided by copyright and licenses.

8. Do inform the I.T. Department immediately of any unusual occurrence.

DO NOT

9. Do not download text or images which contain material of a pornographic, racist or extreme political nature, or which incites violence, hatred or any illegal activity.

10. Do not download content from Internet sites unless it is work related.

11. Do not download software from the Internet and install it upon the Organisation's computer equipment.

12. Do not use the Organisation's computers to make unauthorised entry into any other computer or network.

13. Do not disrupt or interfere with other computers or network users, services, or equipment. Intentional disruption of the operation of computer systems and networks is a crime under the Computer Misuse Act 1990.

14. Do not represent yourself as another person.

15. Do not use Internet access to transmit confidential, political, obscene, threatening, or harassing materials.

Please note the following

All activity on the Internet is monitored and logged.
All material viewed is scanned for viruses.
All the content viewed is scanned for offensive material.

If you are in any doubt about an issue affecting Internet Access you should consult the I.T. Department.

Any breach of the Organisation's Internet Acceptable Use Policy may lead to disciplinary action.

2. Chính sách sử dụng email

- Sử dụng email bởi các nhân viên của tổ chức cần được cho phép và khuyến khích (sử dụng email nhằm hỗ trợ các mục tiêu và mục đích của tổ chức).

2. Chính sách sử dụng email

- Tuy nhiên, các tổ chức khi ban hành chính sách sử dụng email cho nhân viên cần phải bảo đảm:
  - Tuân thủ luật pháp hiện hành
  - Sử dụng email một cách chấp nhận được
  - Không tạo ra rủi ro kinh doanh không cần thiết cho công ty
  - Không chuyển những thông tin bí mật của công ty ra ngoài
  - Sử dụng các hệ thống truyền thông của công ty, bao gồm email để thiết lập các hoạt động kinh doanh cho cá nhân.

Chính sách sử dụng email

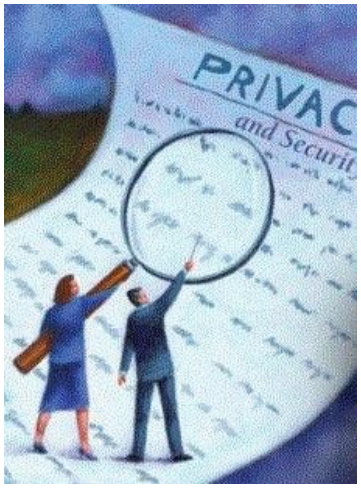
- Phân phối, phổ biến hoặc tàng trữ hình ảnh, văn bản hoặc các tài liệu mà phi pháp.
- Sử dụng thông tin vi phạm quyền tác giả
- Đột nhập vào hệ thống của công ty hoặc tổ chức khác hoặc sử dụng trái phép mật khẩu/ hộp thư
- Truyền tải các quan điểm cá nhân về các vấn đề liên quan tới chính trị, tôn giáo hoặc các vấn đề liên quan khác.

Chính sách sử dụng email

- Phỉ báng, nói xấu và/hoặc phát tán tài liệu sai về tên DN, đồng nghiệp và/hoặc các khách hàng trên mạng xã hội, diễn đàn và bất kỳ dạng xuất bản trực tuyến khác.

3. Bí mật riêng tư/Privacy đến AUP

- Quyền độc lập cá nhân và quyền tự do từ các xâm phạm cá nhân không hợp lý.
- Thông tin cá nhân được thu thập:
  - Đăng kí sử dụng dịch vụ điện tử
  - Đăng kí thành viên,
  - Mua hàng
  - Cookies
  - Phần mềm gián điệp (Spyware)
  - …



Bí mật riêng tư/Privacy đến AUP

- **Chính sách bảo mật thông tin khách hàng** là một tài liệu văn bản gồm các quy định về việc thu thập, sử dụng, tiết lộ dữ liệu thông tin cá nhân .
- Đối với website TMĐT, chính sách bảo mật thông tin khách hàng là một tài liệu văn bản điện tử có nhiều quy định, đăng tải trên website nhằm thông báo cho khách hàng và những người truy cập website về mục đích của việc thu thập thông tin, những thông tin được thu thập, sử dụng thông tin, chia sẻ thông tin…

Bí mật riêng tư/Privacy đến AUP

Bản chất của chính sách bảo mật thông tin khách hàng:

- Là tuyên bố của chủ website đối với khách hàng hoặc người truy cập.
- Là một loại quy định mặc định một phía trong hợp đồng giao dịch mà những người truy cập website TMĐT phải nên biết trước và tuân thủ.

Bí mật riêng tư/Privacy đến AUP

Bản chất của chính sách bảo mật thông tin khách hàng:

- Thường bao gồm các nhóm quy định về: (1) phương pháp thu thập thông tin khách hàng/người dùng; (2) loại thông tin được thu thập; (3) mục đích thu thập thông tin; (4) chia sẻ và tiết lộ thông tin; (5) thay đổi hoặc sửa đổi thông tin.

Bí mật riêng tư

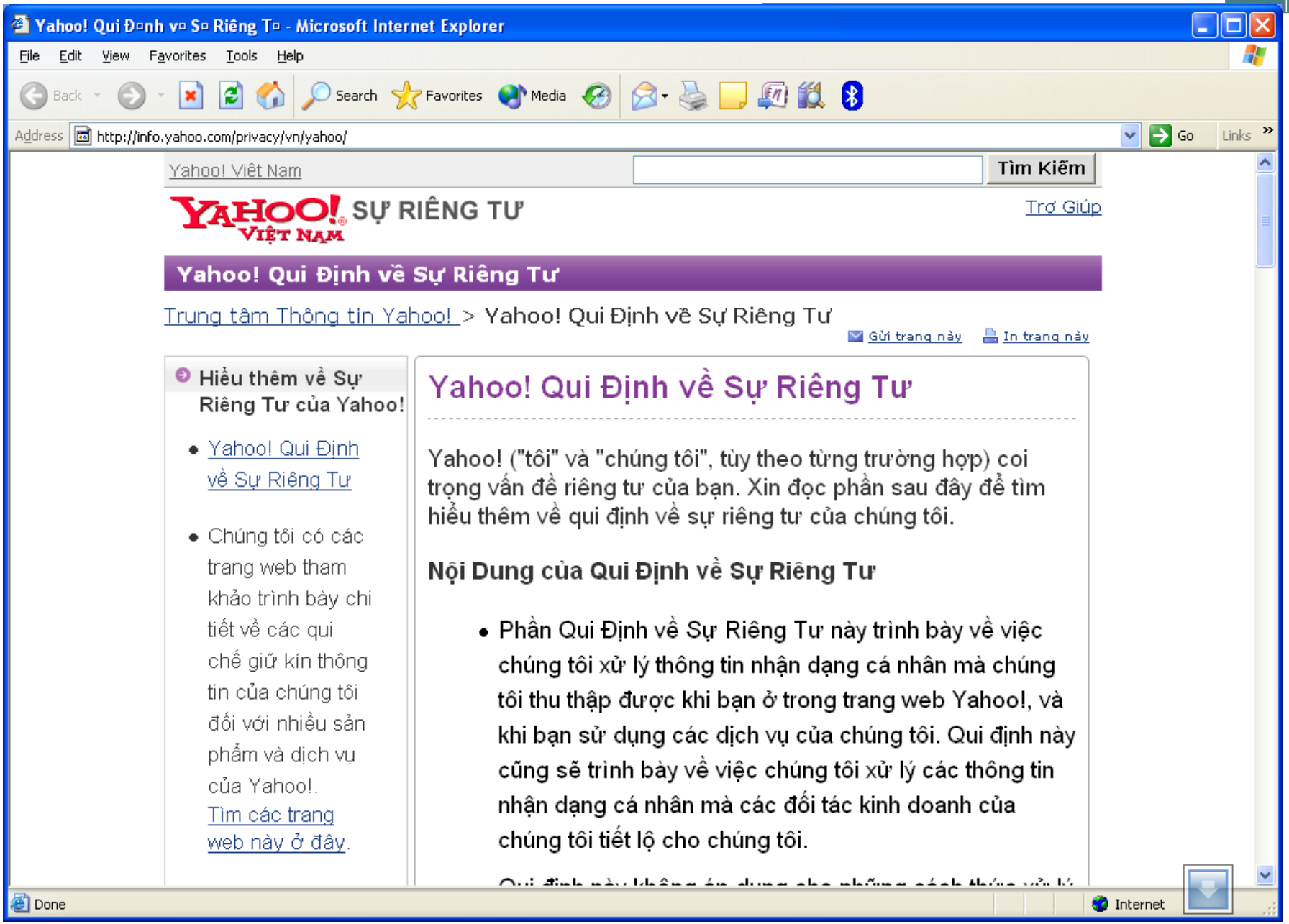
- Đạo luật yêu nước của Mỹ (USA Patriot Act)
  - Gia tăng (Dramatic increases in the scope) và hình phạt của các gian lận máy tính và hành vi lạm dụng
  - Mở rộng thẩm quyền của cơ quan giám sát/cơ quan tình báo FISA (Foreign Intelligence Surveillance Act)
  - Tăng cường chia sẻ thông tin giữa lực lượng thực thi pháp luật địa phương và cơ quan tình báo
  - Cơ quan tình báo (FISA) giám sát những hạn chế của cơ quan địa phương và cơ quan địa phương giám sát hạn chế của cơ quan tình báo.

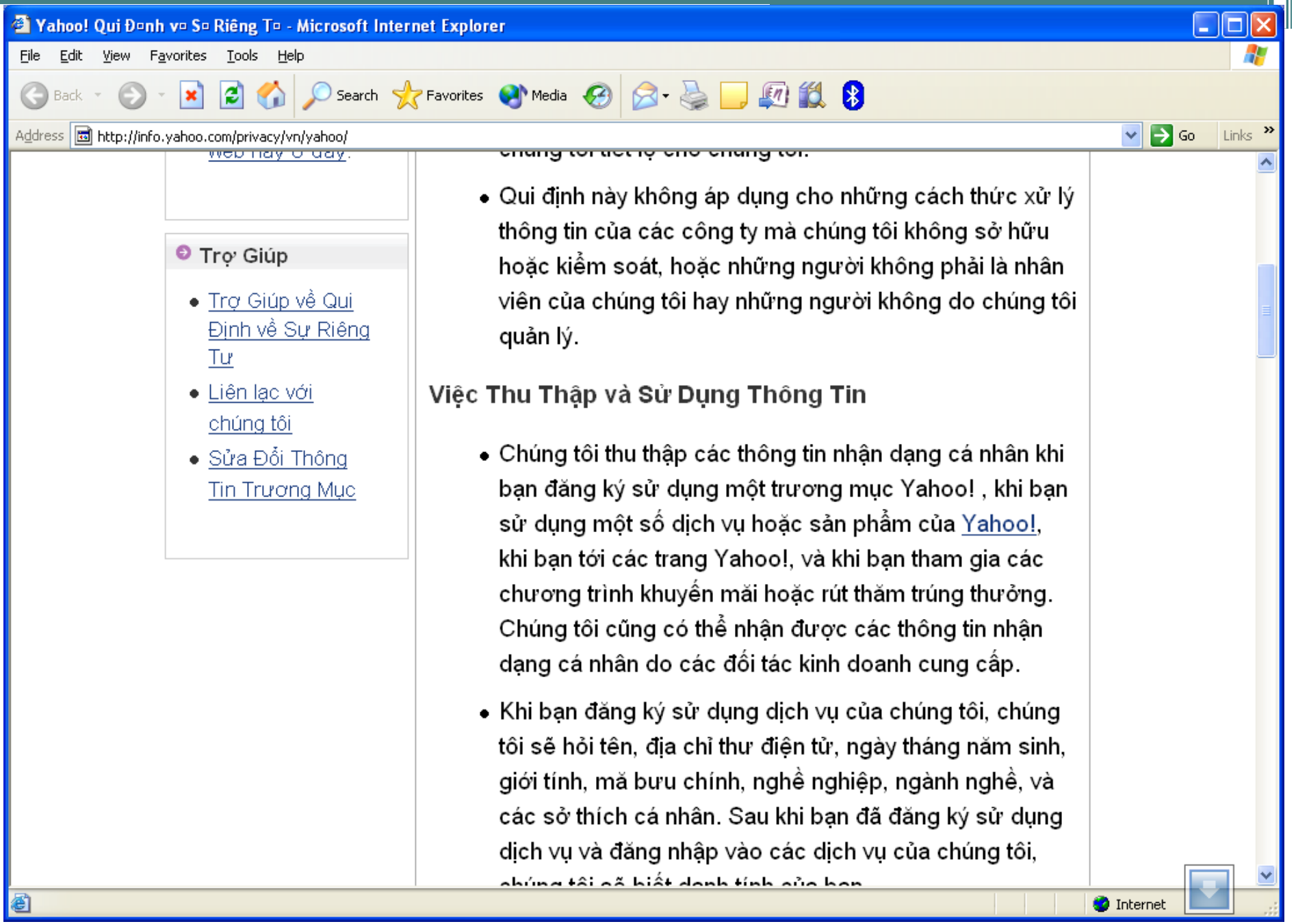
Bí mật riêng tư

- Luật bảo vệ trẻ em trực tuyến (COPA): tiếp cận phương pháp bảo vệ con người
- Ví dụ: luật chống game của bang California, Mỹ, với những quy định cấm bán hoặc cho thuê game có nội dung bạo lực đối với trẻ vị thành niên. Trong năm 2005, lần lượt hai bang Illinois và Michigan đã thông qua lệnh cấm bán các trò chơi video có tính chất bạo lực và khiêu dâm cho trẻ em.

Bí mật riêng tư

- Bảo vệ bí mật riêng tư ở nước ngoài
  - Năm 1998, Ủy ban Châu Âu đã thông qua một *hướng dẫn bí mật riêng tư* (EU Data Protection Directive) xác nhận lại những nguyên tắc của bảo vệ dữ liệu cá nhân trong thời đại internet.
  - *Hướng dẫn* có mục đích điều chỉnh các hoạt động của bất kì cá nhân hoặc công ty có liên quan tới việc thu thập, lưu trữ, xử lí hoặc sử dụng dữ liệu cá nhân trên mạng internet.


Yahoo! Qui Đ▫nh v▫ S▫ Riêng T▫ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://info.yahoo.com/privacy/vn/yahoo/
Go Links
Yahoo! Việt Nam
Tìm Kiếm
YAHOO! VIỆT NAM SỰ RIÊNG TƯ
Trợ Giúp
Yahoo! Qui Định về Sự Riêng Tư
Trung tâm Thông tin Yahoo! > Yahoo! Qui Định về Sự Riêng Tư
Gửi trang này
In trang này
Hiểu thêm về Sự Riêng Tư của Yahoo!
Yahoo! Qui Định về Sự Riêng Tư
Chúng tôi có các trang web tham khảo trình bày chi tiết về các qui chế giữ kín thông tin của chúng tôi đối với nhiều sản phẩm và dịch vụ của Yahoo!. Tìm các trang web này ở đây.
Yahoo! Qui Định về Sự Riêng Tư
Yahoo! ("tôi" và "chúng tôi", tùy theo từng trường hợp) coi trọng vấn đề riêng tư của bạn. Xin đọc phần sau đây để tìm hiểu thêm về qui định về sự riêng tư của chúng tôi.
Nội Dung của Qui Định về Sự Riêng Tư
Phần Qui Định về Sự Riêng Tư này trình bày về việc chúng tôi xử lý thông tin nhận dạng cá nhân mà chúng tôi thu thập được khi bạn ở trong trang web Yahoo!, và khi bạn sử dụng các dịch vụ của chúng tôi. Qui định này cũng sẽ trình bày về việc chúng tôi xử lý các thông tin nhận dạng cá nhân mà các đối tác kinh doanh của chúng tôi tiết lộ cho chúng tôi.
Done
Internet


Yahoo! Qui Đ▫nh v▫ S▫ Riêng T▫ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://info.yahoo.com/privacy/vn/yahoo/
Go Links
Web này ở đây.
Trợ Giúp
Trợ Giúp về Qui Định về Sự Riêng Tư
Liên lạc với chúng tôi
Sửa Đổi Thông Tin Trương Mục
chúng tôi tiết lộ cho chúng tôi.
Qui định này không áp dụng cho những cách thức xử lý thông tin của các công ty mà chúng tôi không sở hữu hoặc kiểm soát, hoặc những người không phải là nhân viên của chúng tôi hay những người không do chúng tôi quản lý.
Việc Thu Thập và Sử Dụng Thông Tin
Chúng tôi thu thập các thông tin nhận dạng cá nhân khi bạn đăng ký sử dụng một trương mục Yahoo! , khi bạn sử dụng một số dịch vụ hoặc sản phẩm của Yahoo!, khi bạn tới các trang Yahoo!, và khi bạn tham gia các chương trình khuyến mãi hoặc rút thăm trúng thưởng. Chúng tôi cũng có thể nhận được các thông tin nhận dạng cá nhân do các đối tác kinh doanh cung cấp.
Khi bạn đăng ký sử dụng dịch vụ của chúng tôi, chúng tôi sẽ hỏi tên, địa chỉ thư điện tử, ngày tháng năm sinh, giới tính, mã bưu chính, nghề nghiệp, ngành nghề, và các sở thích cá nhân. Sau khi bạn đã đăng ký sử dụng dịch vụ và đăng nhập vào các dịch vụ của chúng tôi,
Internet

CHÍNH SÁCH ĐẢM BẢO AN TOÀN THÔNG TIN CÁ NHÂN TRÊN TRANG TIN ĐIỆN TỬ CỦA UỶ BAN DÂN TỘC

Trang thông tin điện tử của Ủy ban Dân tộc trên mạng Internet về lĩnh vực công tác dân tộc tại địa chỉ http://www.cema.gov.vn (gọi tắt là Website CEMA) được Cục Báo chí – Bộ Văn hóa Thông tin (nay là Cục Quản lý Phát thanh Truyền hình và Thông tin điện tử thuộc Bộ Thông tin và Truyền thông) cấp trong giấy phép số: 455/GP-BC ngày 18/10/2004.

Nhằm đảm bảo an toàn cho Website CEMA, đồng thời bảo mật thông tin khách hàng, Website CEMA đưa ra Chính sách bảo mật thông tin cá nhân (Privacy Policy) dành cho các tổ chức và cá nhân truy cập website. Thuật ngữ "Bạn" được dùng trong văn bản này

4. Những nguyên tắc cơ bản về bảo vệ dữ liệu cá nhân trong TMĐT

- **Nguyên tắc 1**: Ngăn ngừa thiệt hại

Mục tiêu: là ngăn ngừa việc sử dụng bất hợp pháp dữ liệu cá nhân cũng như những thiệt hại phát sinh.

Bảo vệ dữ liệu cá nhân

Các biện pháp chế tài xử lý vi phạm về bảo vệ dữ liệu cá nhân cần được xây dựng phù hợp với mức độ thiệt hại từ việc thu thập hoặc sử dụng thông tin trái phép

- **Nguyên tắc 2**: Thông báo trước
- **Nguyên tắc 3**: Giới hạn phạm vi thu thập dữ liệu cá nhân
- **Nguyên tắc 4**: Sử dụng dữ liệu cá nhân
- **Nguyên tắc 5**: Quyền lựa chọn của chủ thể dữ liệu cá nhân
- **Nguyên tắc 6**: Tính toàn vẹn của dữ liệu cá nhân
- **Nguyên tắc 7**: An ninh, an toàn dữ liệu cá nhân
- **Nguyên tắc 8**: Tiếp cận và điều chỉnh dữ liệu cá nhân
- **Nguyên tắc 9**: Trách nhiệm

NgânLượng.vn
Trung tâm hỗ trợ khách hàng

NEW NgânLượng.vn TỰ HÀO LÀ SỐ MỘT với 24 điểm khác biệt

TRUNG TÂM TRỢ GIÚP | QUY ĐỊNH - CHÍNH SÁCH | HƯỚNG DẪN NGÂNLƯỢNG.VN | HƯỚNG DẪN PAYPAL | HƯỚNG DẪN TÍCH HỢP

Trang chủ → Quy định - Chính sách → Quyền riêng tư

Nhập từ khóa...

- Thỏa thuận người dùng
- Khiếu nại và bảo hiểm giao dịch
- Thỏa thuận Merchant
- Chính sách điểm tích lũy
- Quyền riêng tư

LIÊN HỆ TRỰC TIẾP VỚI CHÚNG TÔI

Hotline: **0984-863-761**
Hà Nội: **1900-5858-99**
TP.HCM: **(08) 6292 0945**
Email: **support@nganluong.vn**
Hỗ trợ chung
Hỗ trợ kỹ thuật

Chính sách quyền riêng tư (Privacy Policy)

Chính sách này có mã phiên bản 2.0, được làm và công bố ban hành ngày 01/06/2010 tại Công ty Cổ phần Giải pháp Phần mềm Hòa Bình, pháp nhân chủ quản cổng thanh toán trực tuyến trung gian NgânLượng.vn.

Bạn là người dùng có tài khoản thanh toán mở tại NgânLượng.vn, mặc nhiên chấp nhận nội dung chính sách này với những điều cụ thể sau đây.

Điều 1: Thu thập thông tin

NgânLượng.vn sẽ thu thập địa chỉ IP và các thông tin web tiêu chuẩn khác của bạn như: loại trình duyệt, các trang bạn truy cập trong quá trình sử dụng dịch vụ, thông tin về máy tính & thiết bị mạng v.v... cho mục đích bảo mật & an toàn giao dịch.

Nếu bạn mở tài khoản thanh toán, chúng tôi sẽ yêu cầu bạn cung cấp trung thực & chính xác những thông tin sau:

- Thông tin nhân thân & liên hệ (đối với tổ chức & cá nhân) như: tên, ngày sinh, giới tính, địa chỉ, điện thoại, email, giấy tờ hợp pháp (như CMTND, GPKD, ĐK MST) v.v...
- Thông tin tài chính như số tài khoản ngân hàng, số thẻ ghi nợ hoặc thẻ tín dụng v.v...

Trong một số trường hợp, chúng tôi có thể thu thập thêm thông tin về bạn từ bên thứ ba như ngân hàng, các tổ chức tín dụng & dịch vụ thanh toán, nhà cung cấp dịch vụ mạng v.v...

Chúng tôi cũng có thể thu thập thêm các thông tin khác về bạn từ nhiều nguồn & bằng các phương thức khác nhằm đảm bảo chất lượng dịch vụ và phục vụ bạn tốt hơn.

Điều 2: Đặt Cookies

Khi bạn truy cập NgânLượng.vn, chúng tôi (hoặc bên thứ ba được thuê để theo dõi hoặc thống kê hoạt động của website) sẽ đặt một số File dữ liệu nhỏ gọi là Cookies lên đĩa cứng hoặc bộ nhớ máy tính của bạn. Một trong số những Cookies này có thể tồn tại lâu để thuận tiện cho bạn trong quá trình sử dụng, ví dụ như: lưu Email của bạn trong trang đăng nhập để bạn không phải nhập lại v.v…Chúng tôi sẽ mã hóa các File Cookies để bảo mật, bạn có thể cấm Cookies trên trình duyệt của mình nhưng điều này có thể ảnh hưởng đến quá trình sử dụng NgânLượng.vn của bạn.

Điều 3: Lưu trữ & Bảo vệ thông tin

Chúng tôi lưu trữ và xử lý thông tin cá nhân của bạn tại các máy chủ đặt tại Việt Nam. Chúng tôi bảo vệ những thông tin này bằng nhiều phương tiện bảo vệ vật lý (ví dụ: kiểm soát ra vào tòa nhà có chứa máy chủ), điện tử (ví dụ: tường lửa, mã hóa dữ liệu) và quy trình làm việc của đội ngũ nhân viên vận hành.

4. Chuẩn an ninh thông tin

- ISO/IEC 27001 là một tiêu chuẩn quốc tế cung cấp một khuôn khổ để thực hành thông tin an toàn.
- Các lĩnh vực được bao hàm bởi ISO/ IEC 27001 ISO/IEC 27001:2005 – Specification
  - Specifies requirements for establishing, implementing, and documenting Information Security Management Systems (ISMS)
  - Specifies requirements for security controls to be implemented according to the needs of individual organizations
  - Consists of 11 control sections, 39 control objectives, and 133 controls
  - Is aligned with ISO/IEC 17799:2005

Development of ISO/IEC 270001 "family" of standards

ISO/IEC Standard	Description
27000	Vocabulary and definitions
27001	Specification (BS7799-2) Issued October 2005
27002	Code of Practice (ISO17799:2005)
27003	Implementation Guidance
27004	Metrics and Measurement
27005	Risk Management (BS 7799-3)

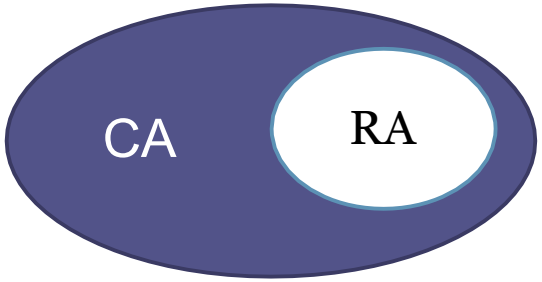
Các vấn đề chính đối với tiêu chuẩn ISO / IEC 27001: 2005

- Tích hợp các quy trình và chính sách an toàn CNTT vào quy định hiện tại của tổ chức
- Thực hiện một phương tiện để tuân thủ và cải tiến liên tục (Implements a means for continuous compliance and improvement)
- Củng cố, tăng cường an ninh an toàn CNTT như là một phần của quản trị doanh nghiệp tốt (Reinforces IT security as part of good corporate governance)
- Xây dựng các chuẩn được quốc tế chấp nhận (Built on internationally accepted standards)

Chương 6
Thương mại điện tử Việt Nam và những vấn đề trở ngại

NỘI DUNG

1. Khái quát kiểm soát RR TMĐT
2. Các biện pháp quản trị RR an toàn TT
3. Các biện pháp xử lý rủi ro khác



1. Khái quát kiểm soát RR TMĐT

Phân tích rủi ro (Risk Analysis)

- Là nhận biết, đánh giá khả năng của tất cả RR tiềm ẩn và tác động đến tổ chức nếu đe dọa xảy ra. Để phân tích RR, các đe dọa cần được phân tích riêng. Mặc dù có thể có nhiều đe dọa đến các hệ thống, bộ phận khác nhau, hệ thống máy chủ có thể là RR cao nhất, nhưng nó không phải là mối quan tâm duy nhất.

1. Khái quát kiểm soát RR TMĐT (tiếp..)

Phân tích rủi ro (Risk Analysis)

- Là thực hiện đánh giá toàn diện và chi tiết các RR tiềm ẩn và các lỗ hổng bảo mât, tính toàn vẹn, tính sẵn sàng của các thông tin…
- Là việc xác định, đánh giá và xếp hạng các RR với mục đích tiết kiệm các nguồn lực cũng như giảm thiểu kiểm soát, tổn thất và tác động không mong muốn và tối đa hóa việc thực hiện các cơ hội, bao gồm:

Những khái niệm liên quan kiểm soát RR TMĐT

Quy trình phân tích rủi ro

- Xác định phạm vi, mục tiêu các đối tượng cần bảo vệ (Map Objectives)
- Nhận biết các đe dọa, tấn công (ID threats)
- Đánh giá lỗ hổng (Assess Vulnerabilities
- Xác định xác suất xảy ra (Determine Risk Likelihood
- Xác định tổn hại (Determine Threat Impact)
- Xác định cấp độ RR (Determine Level or Risk)
- Lập hồ sơ (Documentation)

PP định tính phân tích RR

Theo tần xuất xuất hiện của RR: có 4 mức qua ước lượng sự quan trọng của nó.

- Mức thường xuyên
- Mức hay xảy ra
- Mức đôi khi, thỉnh thoảng
- Mức hiếm (ít) khi

PP định tính phân tích RR

Theo thời điểm xuất hiện/xảy ra: có 4 mức để ước lượng thời điểm rủi ro xuất hiện, tùy sự tác động của nó.

- Mức ngay lập tức
- Mức rất gần
- Mức sắp xảy ra
- Mức rất lâu

Ví dụ: phân tích tình huống website du lịch bị tấn công DOS vào các thời điểm: mùa du lịch, các mùa khác; giả dụ thời gian bị tấn công 3 h

Các nguyên tắc phân tích RR theo OWASP

- OWASP (The Open Web Application Security Project) đề xuất các nguyên tắc phân tích RR, mức điểm từ 0 - 9, với đánh giá xác suất xảy ra trên hai yếu tố

1. **Yếu tố đe dọa:**

   - ***Mức độ kĩ năng đe dọa (Skill level):*** nhóm đe dọa có kĩ năng đe dọa ntn?
     - Không có kĩ năng (1),
     - Một số kĩ năng (3),
     - Có nhiều kĩ năng dùng máy tính (4),
     - Kĩ năng lập trình và mạng (6),
     - Kĩ năng truy nhập bảo mật (9)

Các nguyên tắc phân tích RR theo OWASP

1. **Yếu tố đe dọa:**

Động cơ (Motive): của phát hiện, tìm ra lỗ hổng là gì?

- Không vì được phần thưởng, lợi ích (1),
- Có thể được phần /khen thưởng (4),
- Được khen thưởng, vụ lợi (9)

Các nguyên tắc phân tích RR theo OWASP

- ***Cơ hội, thời cơ (Opportunity):*** những nguồn lực và cơ hội nào cần thiết để tấn công khai thác lỗ hổng xảy ra
  - full access or expensive resources required (0),
  - special access or resources required (4),
  - some access or resources required (7),
  - no access or resources required (9)

Các nguyên tắc phân tích RR theo OWASP

- ***Quy mô (Size):*** How large is this group of threat agents?
  - Developers (2),
  - system administrators (2),
  - intranet users (4),
  - partners (5),
  - authenticated users (6),
  - anonymous Internet users (9)

Phân tích RR theo mức độ

2. Yếu tố lỗ hổng (Vulnerability factors)

- ***Dễ phát hiện lỗ hổng (Ease of discovery):***
  - Practically impossible (1),
  - difficult (3),
  - easy (7),
  - automated tools available (9)
- ***Dễ khai thác lỗ hổng (Ease of exploit):***
  - Theoretical (1),
  - difficult (3),
  - easy (5),
  - automated tools available (9)

Phân tích RR theo mức độ

2. Yếu tố lỗ hổng (Vulnerability factors)

- ***Nhận thức (Awareness):***
  - Unknown (1),
  - hidden (4),
  - obvious (6),
  - public knowledge (9)
- ***Phát hiện xâm nhập (Intrusion detection):***
  - Active detection in application (1),
  - logged and reviewed (3),
  - logged without review (8),
  - not logged (9)

Phân tích RR theo mức độ

Đánh giá tổn thất theo thang điểm từ 0 – 9

- Tổn thất về kĩ thuật: được xem xét là: tính bí mật C, tính sẵn sàng A và tính toàn vẹn I, tính trách nhiệm Accountability. Mục đích là ước tính độ lớn trên hệ thống nếu lỗ hổng bị khai thác.
  - ***Tổn thất tính bí mật***: Dữ liệu bị tiết lộ, và dữ liệu nhạy cảm.
    - Dữ liệu bị tiết lộ rất nhỏ (2),
    - Dữ liệu quan trọng bị tiết lộ rất nhỏ (6),
    - Dữ liệu bị tiết lộ mở rộng (6)

Phân tích RR theo mức độ

- Dữ liệu quan trọng bị tiết lộ mở rộng (7),
- Tất cả dữ liệu bị tiết lộ (9)

- ***Tổn thất tính toàn vẹn***: Bao nhiêu dữ liệu bị chiếm giữ và thiệt hại?
  - Một số dữ liệu bị chiếm giữ (1),
  - Một số dữ liệu quan trọng bị chiếm giữ (3),
  - Một số lớn dữ liệu bị chiếm giữ (5),
  - Một số lớn dữ liệu quan trọng bị chiếm giữ (7),
  - Tất cả dữ liệu bị chiếm giữ (9)

Phân tích RR theo mức độ

Đánh giá tổn thất theo thang điểm từ 0 – 9

- ***Tổn thất tính sẵn sàng***: Bao nhiêu dịch vụ bị mất và mức quan trọng của dịch vụ đó?
  - Một số DV bổ sung bị gián đoạn (1),
  - Một số DV chủ yếu bị gián đoạn (5),
  - Các DV bổ sung bị gián đoạn mở rộng (5),
  - Các DV chính bị gián đoạn mở rộng (7),
  - Tất cả các DV bị đứt, ngưng (9)

Phân tích RR theo mức độ

Đánh giá tổn thất theo thang điểm từ 0 – 9

- ***Tổn thất trách nhiệm***: liệu các hành động tác nhân đe dọa có thể theo dõi tới một cá nhân mức độ?
  - Hoàn toàn theo dõi (1),
  - Chỉ có thể theo dõi (7),
  - Hoàn toàn vô danh không thể theo dõi (9)

Phân tích RR theo mức độ

Đánh giá tổn thất theo thang điểm từ 0 – 9

- ***Thiệt hại uy tín, danh tiếng (Reputation damage)***: Thiệt hại tối thiểu (1), Mất các tài khoản chính (4), Mất uy tín – goodwill (5), Thiệt hại thương hiệu - brand damage (9)
- ***Sự chối bỏ (Non-compliance)***: Vi phạm nhỏ (2), Vi phạm rất lớn (7)

Phân tích RR theo mức độ

Đánh giá tổn thất theo thang điểm từ 0 – 9

- ***Vi phạm bí mật riêng tư (Privacy violation):*** Thông tin cá nhân bị tiết lộ như thế nào? Một cá nhân (3), hàng trăm người (5), hàng nghìn người (7), hàng triệu người (9)
- ***Thiệt hại tài chính***: tổn thất tài chính là bao nhiêu tiền? Thấp hơn chi phí vá lỗ hổng (1), ảnh hưởng nhỏ tới lợi nhuận cả năm (3), ảnh hưởng lớn đến lợi nhuận cả năm (7), phá sản (9)

PP định lượng phân tích rủi ro RE

- Mức độ rủi ro (RE) là rủi ro được xác định dựa trên giá trị tài sản tổn thất L(o) và khả năng xảy ra tổn thất P(o). Khi đó:

  Mức độ rủi ro: RE = P(O) x L(O)
- Mức độ rủi ro (RE) cũng có thể được xác định dựa trên giá trị của tài sản (A), khả năng xảy ra đe dọa/bị tấn công (T), khả năng khai thác lỗ hổng (V), và mức độ tổn thất (I). Khi đó mức độ rủi ro: RE = A x T x V x I.

Một số câu hỏi gợi ý trong quá trình PT RR

- Mức độ thiệt hại như thế nào?
- Xác suất xảy ra cao hay thấp?
- Mức độ rủi ro có thể chấp nhận?
- Rủi ro được xử lí như thế nào?
- Nguyên nhân của rủi ro?
- Có điểm tương đồng giữa các rủi ro?
- Có phụ thuộc vào mối quan hệ?
- What are the risk drivers?

Kiểm soát RR TMĐT

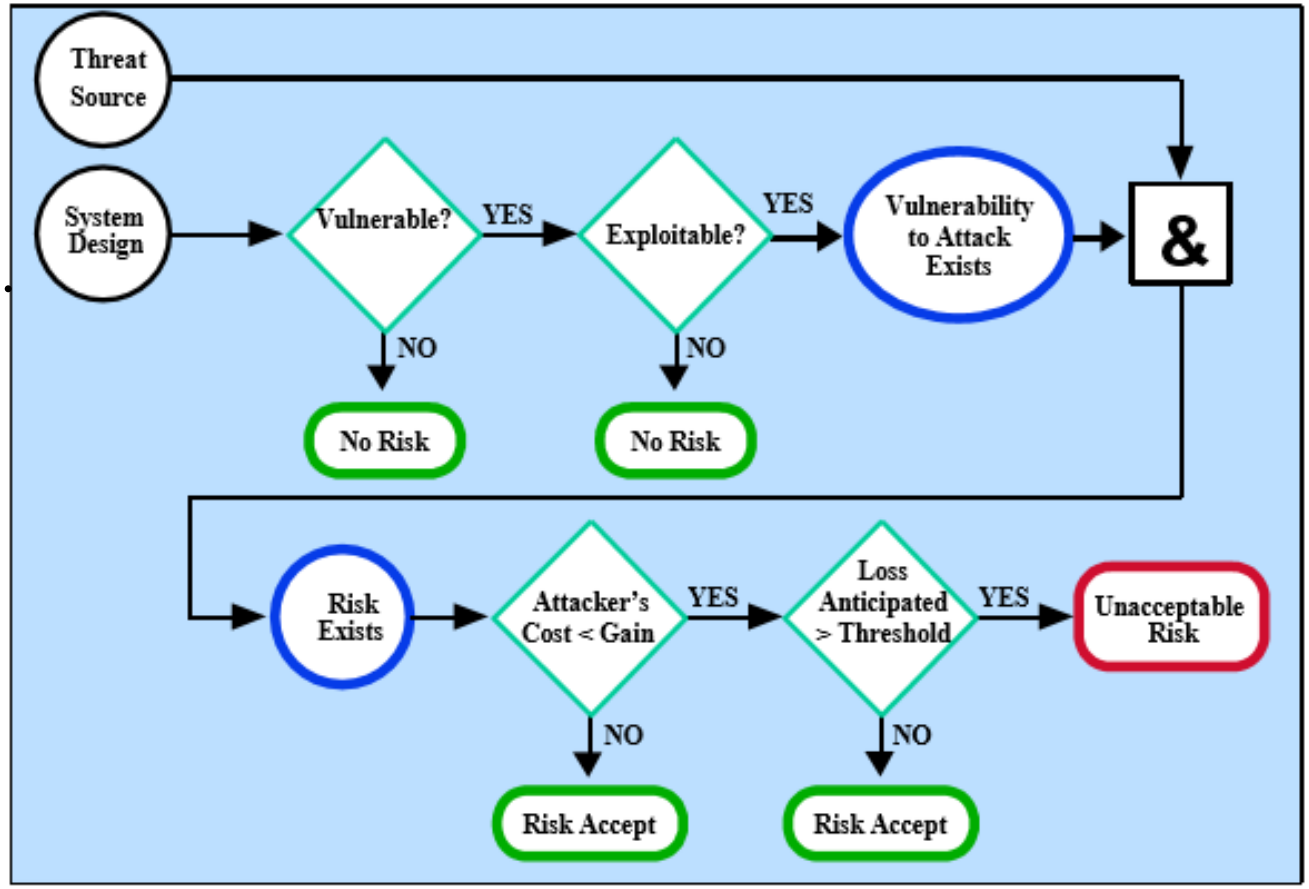
- **Kiểm soát RR** là quá trình thực hiện các biện pháp để ngăn chặn hoặc giảm thiểu rủi ro có thể xảy ra đối với một công việc, hoạt động, quá trình hoặc tài sản.
- Quá trình kiểm soát RR được thực hiện theo phân cấp quản lý và tuân thủ các quy trình kỹ thuật. Điều quan trọng là quá trình kiểm soát rủi ro không tạo ra những mối nguy hiểm mới, và hiệu quả của các kiểm soát được theo dõi liên tục.

Kiểm soát RR TMĐT

- Kiểm soát rủi ro bắt đầu với việc chọn lựa chiến lược và phương pháp đối phó rủi ro. Có nhiều chiến lược và phương pháp đối phó khác nhau, tùy theo từng tình huống, môi trường và đặc thù của từng rủi ro.

Các PP/chiến lược kiểm soát RR

1) Tránh rủi ro,
2) Giảm nhẹ rủi ro,
3) Chuyển giao
4) Chấp nhận rủi ro.



Các PP/chiến lược kiểm soát RR

- Khi tồn tại lỗ hổng
- Khi một lỗ hổng có thể được thực hiện
- Khi chi phí của kẻ tấn công là nhỏ hơn so với lợi ích có được
- Khi tổn thất là quá lớn

Tránh rủi ro (Risk Avoidance)

Tránh rủi ro (Risk Avoidance): Tránh rủi ro là kỹ thuật QTRR đề cập đến:

- Tiến hành các bước để loại bỏ một nguy hiểm,
- Lựa chọn hoạt động thay thế,

Giảm bớt rủi ro (Risk Reduce)

Giảm nhẹ rủi ro (Risk reduction): là một PP kiểm soát RR có sử dụng các kỹ thuật thích hợp để giảm bớt khả năng xảy ra một sự cố, một hậu quả hoặc cả hai... Thực thi các biện pháp để giảm thiểu khả năng xảy ra RR hoặc giảm thiểu tác động và chi phí khắc phục RR nếu nó xảy ra.

Chuyển giao rủi ro (Risk transfer)

- Chuyển giao RR là một biện pháp của kiểm soát rủi ro, được sử dụng trong quản trị RR để mô tả sự chuyển dịch của gánh nặng RR cho một bên khác.
- Chuyển giao RR bằng cách chia sẻ tổn thất, thiệt hại khi chúng xảy ra.

Ví dụ mua bảo hiểm tài sản

DỊCH VỤ BẢO HIỂM MÁY TÍNH Á ĐÔNG

I. Nội dung

Gói 1: Thực hiện việc bảo hiểm tại trung tâm bảo hiểm Á Đông

- Số lần sửa chữa miễn phí **không giới hạn** tại trung tâm

Gói 2: Thực hiện tận nơi khách hàng

- Số lần **sửa chữa miễn phí lên đến 24 lần** tận nơi khách hàng.

Gói 3: Thực hiện tận nơi khách hàng

- Số lần sửa chữa miễn phí **không giới hạn** tận nơi khách hàng.

Sàn giao dịch TMĐT
ĐÃ ĐĂNG KÝ
với Bộ Công Thương

I. Bảng giá *(Áp dụng từ ngày 01/06/2010)*

Dịch vụ bảo hiểm	Gói 1	Gói 2	Gói 3
Dành cho PC	365.000	420.000	730.000
Dành cho Laptop	395.000	520.000	790.000

Trusted Choice®

* Thẻ Bảo hiểm có giá trị cho 1 đơn vị thiết bị (máy tính, thiết bị ngoại vi)/12 tháng

Chấp nhận rủi ro (Risk Acceptance)

- Chấp nhận RR được sử dụng trong quản trị RR để mô tả một quyết định chấp nhận những hậu quả và khả năng của một RR cụ thể.
- Chấp nhận RR hoặc "sống chung" với RR trong trường hợp chi phí loại bỏ, phòng tránh, làm nhẹ RR quá lớn (lớn hơn chi phí khắc phục tác hại), hoặc tác hại của RR nếu xảy ra là nhỏ hay cực kỳ thấp.

Chấp nhận rủi ro (Risk Acceptance)

(tiếp)

- Việc lựa chọn PP kiểm soát RR nào phụ thuộc vào nhiều yếu tố. Đối với DN, lựa chọn PP kiểm soát RR có thể xem là một chiến lược đối phó hợp lý.
- Hoạt động giám sát RR cũng được thực hiện để bảo đảm các chiến lược đối phó rủi ro được đúng kế hoạch và thực thi chặt chẽ.

2. Các biện pháp quản trị RR an toàn TT (Security countermeasures)

Trong quản trị RR an toàn thông tin, **biện pháp đối phó** là một hành động, thiết bị, thủ tục, hoặc kỹ thuật làm giảm mối đe dọa, một lỗ hổng, hoặc một cuộc tấn công bằng cách loại bỏ hoặc ngăn chặn nó, bằng cách giảm thiểu các tác hại nó có thể gây ra, hoặc bằng cách phát hiện và thông báo để sửa chữa, khắc phục các hành động có thể được thực hiện.

Phân loại biện pháp đối phó

- Chính sách an toàn (security policy)
- An toàn thông tin của tổ chức
- Quản trị tài sản
- An toàn nguồn nhân lực
- An toàn vật lý và môi trường
- Quản trị vận hành và truyền thông
- Phần mềm chống Virus
- Phần mềm Anti keyloggers
- Live CD/USB
- Giám sát, theo dõi mạng
- Automatic form filler programs
- One-time passwords (OTP)
- Security tokens

Phân loại biện pháp đối phó

- Kiểm soát truy cập
- Tiếp nhận, bảo trì và phát triển các hệ thống thông tin
- Quản trị sự cố an toàn thông tin
- Quản trị kinh doanh liên tục
- Tuân thủ pháp luật và nội quy.
- On-screen keyboards
- Phần mềm can thiệp - Keystroke interference softwares
- Nhận biết giọng Speech recognition
- Nhận biết vân tay và cử chỉ nhấp chuột
- Macro expanders/recorders
- Non-technological methods

Ví dụ đối phó với Phishing

Ảnh hưởng, tác hại:

- Lừa dối tiết lộ thông tin
- Cho phép kẻ thù truy cập vào thông tin cá nhân, tổ chức

Biện pháp đối phó:

- Cảnh giác
- Xóa bỏ thư điện tử khả nghi
- Contact your system security point of contact with any questions
- Report any potential incidents
- Tìm kiếm chữ kí số
- Sử dụng IDS để chặn, khóa các địa chỉ IP, tên miền
- Cài đặt và cập nhật phần mềm chống vi rút.

Kiểm soát rủi ro

- **Kiểm soát RR** là biện pháp bảo vệ hoặc đối phó để tránh, phát hiện, chống lại hoặc tối thiểu RR đối với tài sản, thông tin, các hệ thống, hoặc tài sản khác. Kiểm soát giúp giảm nguy cơ hư hỏng hoặc mất mát bằng cách ngăn chặn, làm ngưng, hoặc làm chậm một tấn công, một tài sản.

Kiểm soát rủi ro

- **Phân loại kiểm soát RR**: theo thời gian
  - ***Kiểm soát phòng ngừa (preventive controls)***: Trước sự cố xảy ra, nhằm ngăn chặn một sự cố xảy ra
  - ***Kiểm soát phát hiện (detective controls):*** cùng với sự cố xảy ra, nhằm phát hiện và mô tả một sự cố trong quá trình
  - ***Kiểm soát điều chỉnh (corrective controls)***: sau sự cố, nhằm hạn chế mức độ thiệt hại gây ra bởi sự cố
  - Khác: kiểm soát ngăn chặn (deterrent controls), kiểm soát bồi thường (compensation).

Kiểm soát rủi ro

- **Phân loại kiểm soát RR**: theo đối tượng, có 4 loại
  - Kiểm soát vật lí (Physical controls)
  - Kiểm soát thủ tục (Procedural controls)
  - Kiểm soát kĩ thuật (Technical controls)
  - Kiểm soát tuân thủ quy định (Legal and regulatory or compliance controls)
- **Theo quản lý và vận hành**: 03 loại
  - Kiểm soát kỹ thuật (Technical Security Controls)
  - Kiểm soát quản trị (Management Security Controls)
  - Kiểm soát vận hành (Operational Security Controls)

Kiểm soát kỹ thuật

***Bao gồm 3 loại*: Kiểm soát kĩ thuật hỗ trợ; Kiểm soát kĩ thuật ngăn ngừa; và Kiểm soát kĩ thuật phát hiện và phục hồi**

- ***Kiểm soát kĩ thuật hỗ trợ:***
  - Nhận biết Identification
  - Quản lý Khóa mật mã (Cryptographic Key Management
  - Quản lý an ninh (Security Administration)
  - Bảo vệ hệ thống (System Protections):

Kiểm soát kỹ thuật

- ***Kiểm soát kĩ thuật ngăn ngừa***
  - Xác thực (Authentication)
  - Ủy quyền (Authorization):
  - Thực thi kiểm soát truy cập (Access Control Enforcement)
  - Chống chối bỏ (Nonrepudiation)
  - Kiểm soát truyền thông được bảo vệ (Protected Communications)
  - Giao dịch bí mật (Transaction Privacy)

Kiểm soát vận hành

- ***Kiểm soát vận hành ngăn ngừa***:
  - Cung cấp khả năng sao lưu
  - Thiết lập các thủ tục lưu trữ of -site và an toàn
  - Bảo vệ laptops, PC, máy chủ
  - Bảo vệ tài sản IT từ cháy, nổ, các sự cố môi trường
  - Cung cấp nguồn điện dự phòng
  - Kiểm soát độ ẩm và nhiệt độ thiết bị
- ***Kiểm soát vận hành phát hiện***
  - Cung cấp bảo đảm an toàn vật lý
  - Bảo đảm an toàn môi trường

Các hệ thống phát hiện xâm nhập IDS

- **Hệ thống phát hiện xâm nhập (IDS):** là một thiết bị hoặc phần mềm ứng dụng giám sát hệ thống hoặc hoạt động mạng nhằm phát hiện hiện tượng bất thường, các hoạt động trái xâm nhập phép và hệ thống. IDS có thể phân biệt được những tấn công từ bên trong hay từ bên ngoài.
- IDS phát hiện dựa trên các dấu hiệu đặc biệt về các nguy cơ đã biết hay dựa trên so sánh lưu thông mạng hiện tại với thông số đo đạt chuẩn của hệ thống (baseline) để tìm ra các dấu hiệu khác thường.

3. Các biện pháp xử lý rủi ro khác

- Các biện pháp phi công nghệ
  - Đòn bẩy rủi ro
  - Sử dụng biểu đồ GANTT trong kiểm soát RR
  - Cây quyết định

- Các biện pháp công nghệ

Đòn bẩy rủi ro

- Đòn bẩy rủi ro (Risk leverage) là công cụ sử dụng để so sánh biện pháp đối phó RR nào hiệu quả. Đòn bẩy rủi ro/đòn bẩy giảm rủi ro (Risk Reduction Leverage) là một phương pháp đơn giản đưa ra một giá trị với một biện pháp đối phó, có thể các biện pháp đối phó khác nhau để so sánh.
- RL (RRL) được xác định: RL = Sự thay đổi trong mức độ rủi ro/ Chi phí để thực hiện một biện pháp đối phó
- RL = (Mức độ rủi ro trước khi giảm bớt – Mức độ rủi ro sau khi giảm bớt)/Chi phí của giảm rủi ro.

- Tính mức độ rủi ro (RE) để xác định hiệu quả chi phí hiện thời của một rủi ro, và có thể sử dụng để xếp hạng RR được yêu cầu trong biện pháp đối phó
- RE = xác suất xảy ra x mức độ tổn thất nếu RR xảy ra

Rủi ro	P(O)	L(O)	RE
A	2%	80.000	1600
B	0,1%	1000.000	1000
C	10		

RE lớn nhất biểu thị mức độ RR cao nhất

Loại rủi ro	P(O)	L(O)	RE	RL (RRL) = (RE – RE mới)/TC
C	10%	25.000	2500	

Biện pháp đối phó	Tổng chi phí TC	P(O) mới	L(O) mới	RE mới	
C1	40.000	3%	5.000	150	0,059
C2	30.000	5%	10.000	500	0,067
C3	10.000	8%	15.000	1200	0,13

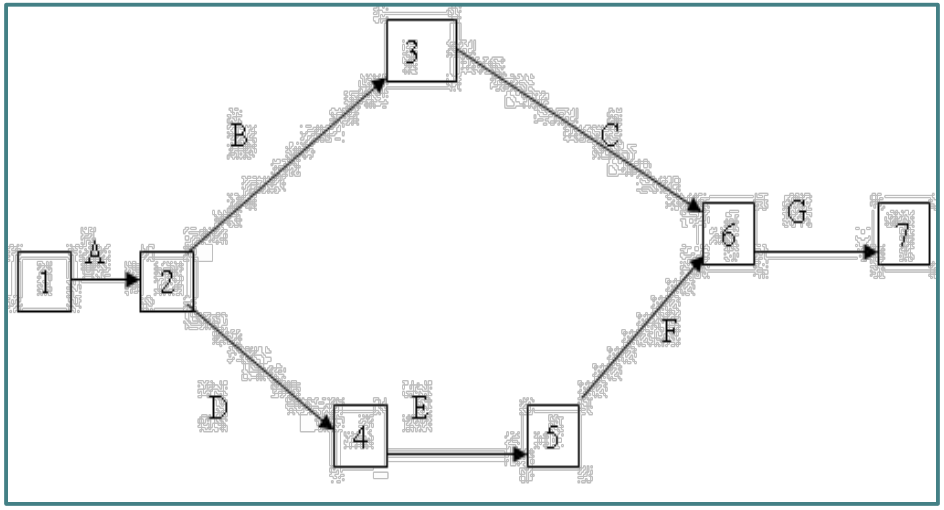
RL lớn nhất biểu thị C3 là biện pháp hiệu quả nhất

Ví dụ

- Ví dụ 1: Mức độ RR trước đối phó là: 5000K; Mức độ RR sau khi can thiệp: 3000K; Chi phí can thiệp RR: 1500K → RRL = (5000K – 3000K)/1500K = 1,33 > 1
- Câu hỏi: Có sử dụng biện pháp can thiệp hay không?
- Trả lời: Đáng làm

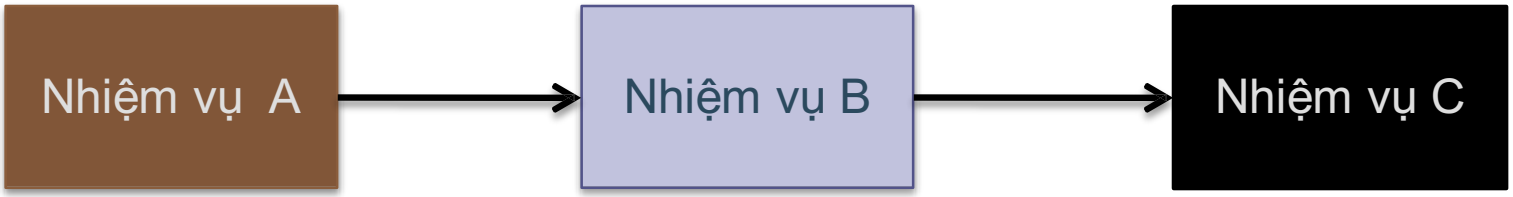
Kỹ thuật kiểm tra và đánh giá việc thực hiện

- Viết tắt là PERT (Performance Evaluation and Review Technique) được phát minh ra năm 1958 khi phát triển tên lửa Polaris . Ban đầu PERT chỉ được dùng để mô tả một dãy các hoạt động qua một tập các mũi tên. Mỗi mũi tên biểu thị cho một hoạt động và được gắn nhãn theo tên hoạt động đó, chẳng hạn A, B, C…



Sử dụng GANTT trong kiểm soát RR

- Ví dụ: một dự án với ba nhiệm vụ thực hiện



Nhiệm vụ	a	m	b	t_e	S
A	10	12	16	?	?
B	8	10	14	?	?
C	20	24	38	?	?

- Thời gian kì vọng hoàn thành dự án: $12.33 + 10.33 + 25.66 = 48.32$
- Sai số chuẩn (độ lệch chuẩn) cho chuỗi nhiệm vụ A + B+ C là:

$$\sqrt{(1^2 + 1^2 + 3^2)} = 3.32$$

Bài toán 1

- **Hãy vẽ sơ đồ PERT cho kế hoạch sau, tô đậm đường Gantt. Chiều dài dự án là bao nhiêu?**

Hoạt động	Thời hạn (ngày)	Hoạt động trước
A	3	-
B	5	A
C	3	A
D	11	B
E	7	B
F	4	C
G	9	E, F
H	2	D, G