TRƯỜNG ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN - VNUHCM - UIT

QUẢN LÝ RỦI RO AN TOÀN THÔNG TIN TRONG DOANH NGHIỆP

Chương 6
Chiến lược quản lý rủi ro

Nội dung

01 Khái quát (General)

02 Các định nghĩa chiến lược (Strategy)

03 Chiến lược QLRR ATTT
(Risk Management Strategy of Information Security)

6.1

Khái quát (General)

6.1.1 Mục đích của doanh nghiệp

6.1.2 Mục tiêu của doanh nghiệp

6.1.3 Mục đích và mục tiêu

6.1 Khái quát (General)(1)

- Một chủ doanh nghiệp khi phát biểu về hoạt động QLRR ATTT trong doanh nghiệp, ông/bà ấy nói là QLRR ATTT:
  - Bảo vệ các giá trị (values) và tài sản của doanh nghiệp;
  - Tập trung nguồn lực vào việc giải quyết những rủi ro ảnh hưởng đến việc đạt được mục tiêu (Objectives);

6.1 Khái quát (General)(2)

- Thiết lập kịp thời các biện pháp kiểm soát (controls) để đảm bảo doanh nghiệp có thể phản ứng nhanh chóng và hiệu quả nếu rủi ro trở thành vấn đề;
- Đảm bảo doanh nghiệp hoạt động liên tục khi đối mặt với sự không chắc chắn ảnh hưởng đến việc hoàn thành mục tiêu

6.1 Khái quát(3)

- Một phát biểu của chủ doanh nghiệp khác về hoạt động QLRR ATTT trong doanh nghiệp, ông/bà ấy nói là QLRR ATTT:
  - Thiết lập và duy trì thời gian gián đoạn hệ thống CNTT không quá 2 giờ/năm;
  - Thiết lập và duy trì thời gian phục hồi hệ thống (Recovery Time Objective - RTO) không quá 30 phút v.v. khi có sự cố ATTT xảy ra;

6.1.1 Mục đích của doanh nghiệp(1)

Mục đích của doanh nghiệp gần với tầm nhìn, sứ mệnh và có:

- Tính chung chung hoặc trừu tượng;
- Tính dài hạn (thời gian thực hiện công việc);
- Thiếu rõ ràng, không cụ thể (về công việc gì phải làm).

: Phát biểu nào trong hai phát biểu như trên là mục đích của doanh nghiệp về hoạt động QLRR ATTT?

6.1.2 Mục tiêu của doanh nghiệp(2)

Mục tiêu (Objective) của doanh nghiệp gần với việc tác nghiệp, có:

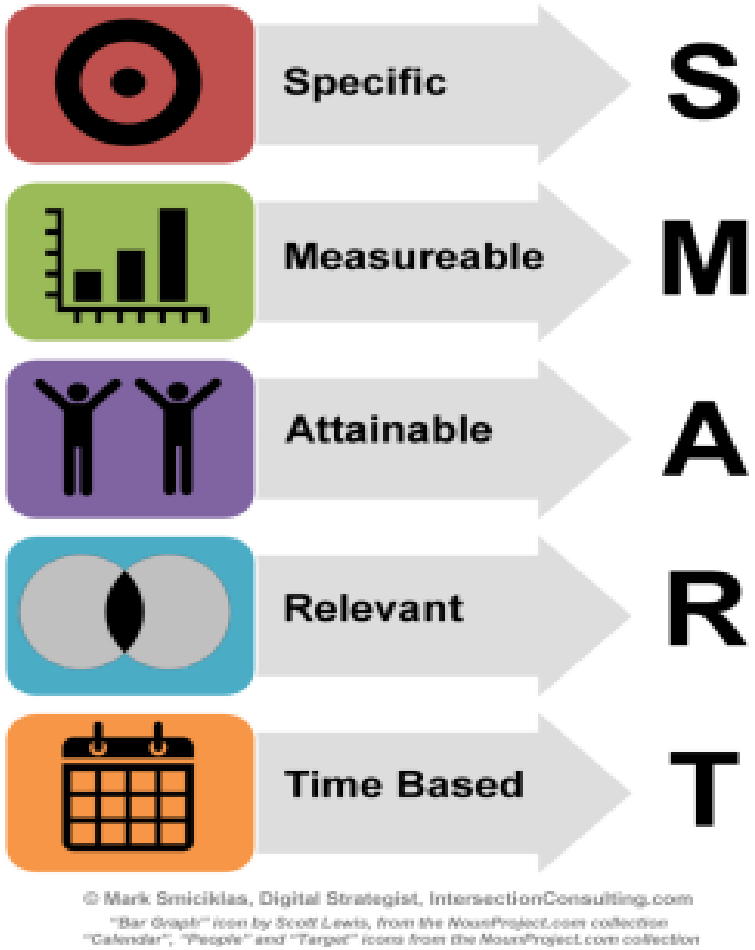
- Tính cụ thể, rõ ràng, chi tiết ('Specific');
- Tính đo lường được ('Measurable');
- Khả năng thực hiện được ('Achievable');
- Tính thực tế ('R-Realistic'); và
- Giới hạn thời gian ('Timebound')

: Phát biểu nào trong hai phát biểu như trên là mục tiêu của doanh nghiệp về hoạt động QLRR ATTT?

6.1.2 Mục tiêu của doanh nghiệp(3)

- S.M.A.R.T là gì?
- Mục đích (purpose) và mục tiêu (Objective)

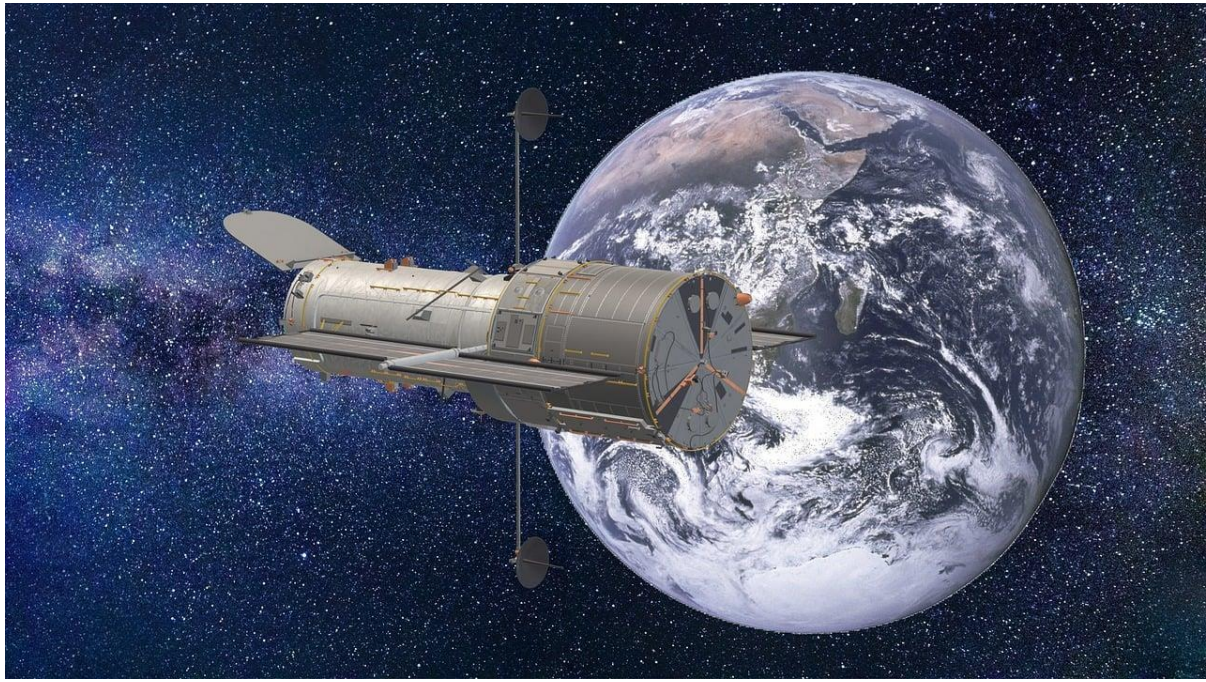
:Cái nào giúp cho việc lập kế hoạch hành động (hay danh sách các công việc cụ thể phải làm) của doanh nghiệp để đạt được kết quả mong muốn?



6.1.3 Mục đích và mục tiêu của doanh nghiệp

- Mục đích (purpose) hay mục tiêu (Objective)?

:Cái nào giúp cho việc lập kế hoạch hành động *(hay danh sách các công việc cụ thể phải làm theo trình tự thời gian)* ***của doanh nghiệp để đạt được kết quả mong muốn?***



6.1.4 Phân biệt mục đích và mục tiêu(1)

- Mục đích (purpose) khác với mục tiêu (Objective):

- Mục đích là lý do tại sao (‘the reason why’) tổ chức tồn tại, tại sao tổ chức làm những gì họ làm, tại sao tổ chức thực hiện hoạt động đó ngay từ đầu;
- Mục đích của tổ chức có tính bao quát, dài hạn, không cụ thể;
- Mục đích được dùng làm cơ sở và biện minh cho mọi hành động được thực hiện(*).

6.1.4 Phân biệt mục đích và mục tiêu(2)

- Mục đích (purpose) khác với mục tiêu (Objective):
  - Mục tiêu là những gì mà tổ chức phải đạt được trong ngắn hạn để đáp ứng một mục đích lớn hơn;
  - Tổ chức theo đuổi một mục tiêu vì nó giúp tổ chức hoàn thành mục đích của mình.
  - Mục tiêu đặt ra phải đáp ứng tiêu chí S.M.A.R.T;

6.2

Các định nghĩa chiến lược

6.2.1 Chiến lược là gì?

6.2.1 Chiến lược kinh doanh của doanh nghiệp

6.2.3 Chiến lược QLRR ATTT và các yêu cầu

6.2.1 Chiến lược là gì?(1)

- **Strategy is an elaborate and systematic plan of action** [ISO 9000]

  (Chiến lược là một kế hoạch hành động chi tiết và có hệ thống)

  - *Systematic: done or acting according to a fixed plan or system; methodical [ISO 9000];*
  - *Plan of action: a detailed set of instructions to follow in order to solve a problem or achieve something (*)*

6.2.1 Chiến lược là gì?(2)

- Strategy is the determination of long-term goals and objectives for the enterprise, the adoption of determined policies and the allocation of resources to reach those goals [Alfred Chandler Jr]

  (Dịch: Chiến lược là việc xác định các mục tiêu dài hạn và mục tiêu ngắn hạn cho doanh nghiệp, thực hiện theo các chính sách đã xác định và phân bổ nguồn lực để đạt được các mục tiêu đó)

6.2.1 Chiến lược là gì?(3)

- Strategy is the creation of a unique and valuable position, involving a different set of activities, and the fit among a company's activities. [Harvard Business Review] *(Chiến lược là việc tạo ra một vị trí độc đáo và có giá trị, bao gồm một loạt các hoạt động khác nhau và sự phù hợp giữa các hoạt động của công ty.)*

6.2.1 Chiến lược là gì?(4)

Chiến lược = Mục tiêu + Kế hoạch hành động

(Strategy) = (Goals and Objectives) + (Plan of Action)

6.2.2 Thiết lập chiến lược kinh doanh (1)

- Chiến lược kinh doanh (hoặc còn gọi là chiến lược hoạt động) là một kế hoạch hành động về kinh doanh của doanh nghiệp;
- Doanh nghiệp thiết lập chiến lược kinh doanh theo 9 bước như sau:

  1. Chi tiết hóa về tầm nhìn và sứ mạng (‘Vision and Mission’);
  2. Thiết lập mục tiêu dài hạn và tổng quát (‘Set goals’);
  3. Thiết lập mục tiêu ngắn hạn, cụ thể, đáp ứng đặc điểm S.M.A.R.T;

(xem slide kế tiếp)

6.2.2 Thiết lập chiến lược kinh doanh(2)

4. Tiến hành xem xét điểm mạnh và điểm yếu của doanh nghiệp (‘Conduct an internal diagnostic’);

5. Tiến hành xem xét cơ hội và mối đe dọa bên ngoài doanh nghiệp (‘Conduct an external diagnostic’);

6.2.2 Thiết lập chiến lược kinh doanh(3)

6. Xác định những chọn lựa có thể (‘Identify possible choices’);

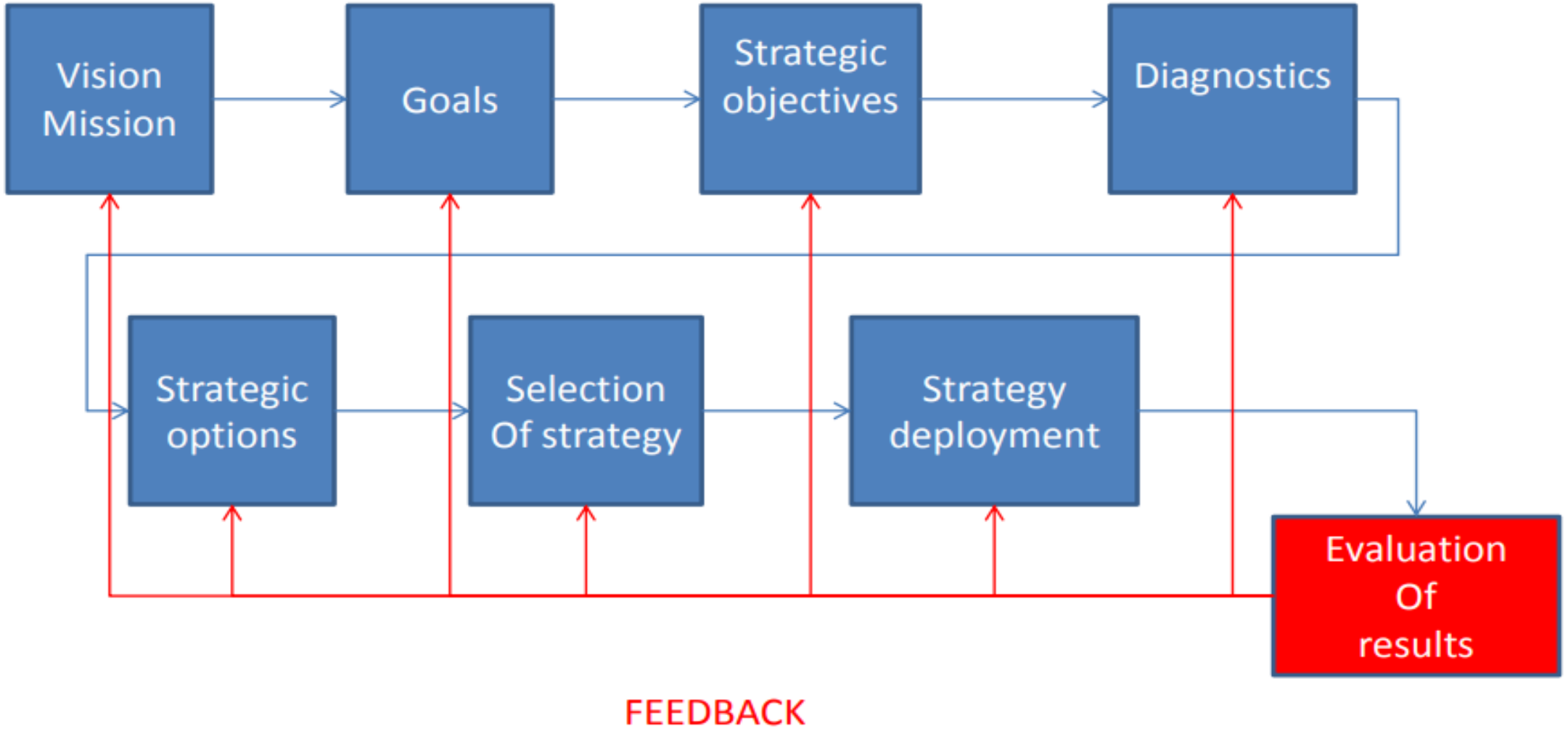
7. Lựa chọn chiến lược (‘Selection of a strategy’);

8. Triển khai chiến lược (‘Deployment of strategy’);

9. Đánh giá kết quả (‘Evaluation of the results’).

Indiana Jones & the last crusade, choose wisely

6.2.2 Thiết lập chiến lược kinh doanh – Quy trình 9 bước



6.2.3 Chiến lược QLRR ATTT và các yêu cầu(1)

- Chiến lược QLRR ATTT là chiến lược đề cập đến cách doanh nghiệp đánh giá rủi ro, ứng phó với rủi ro và giám sát rủi ro.
- Một số ví dụ về chiến lược quản lý rủi ro là chấp nhận rủi ro, giảm thiểu rủi ro, tránh rủi ro và chuyển giao (hay chia sẻ) rủi ro.

CHIẾN LƯỢC = MỤC TIÊU + KẾ HOẠCH HÀNH ĐỘNG

6.2.3 Chiến lược QLRR ATTT và các yêu cầu(2)

Yêu cầu đối với chiến lược QLRR ATTT:

- Phù hợp với nguyên tắc QLRR của doanh nghiệp;
- Phù hợp với mục tiêu và chính sách của doanh nghiệp;
- Phù hợp với chiến lược kinh doanh/hoạt động của doanh nghiệp;
- Phù hợp với tiêu chuẩn quản lý ATTT(ISO 27000 family);
- Đáp ứng tốt nhất sự cân bằng giữa lợi ích và chi phí của doanh nghiệp trước đối thủ cạnh tranh;
- Đáp ứng quyền lợi và nghĩa vụ của các bên liên quan.
- v.v.

6.3

Chiến lược QLRR ATTT (Risk Management Strategy)

6.3.1 Chấp nhận rủi ro

6.3.2 Giảm nhẹ rủi ro

6.3.3 Tránh né rủi ro

6.3.4 Chuyển giao rủi ro

6.3.1 Chấp nhận rủi ro (Risk Acceptance)(1)

- Rủi ro được xem là chấp nhận và không cần phải có biện pháp ứng phó nếu rủi ro còn nằm trong giới hạn cho phép của khẩu vị rủi ro (Risk Appetite); tức là không làm gì cả với rủi ro này.

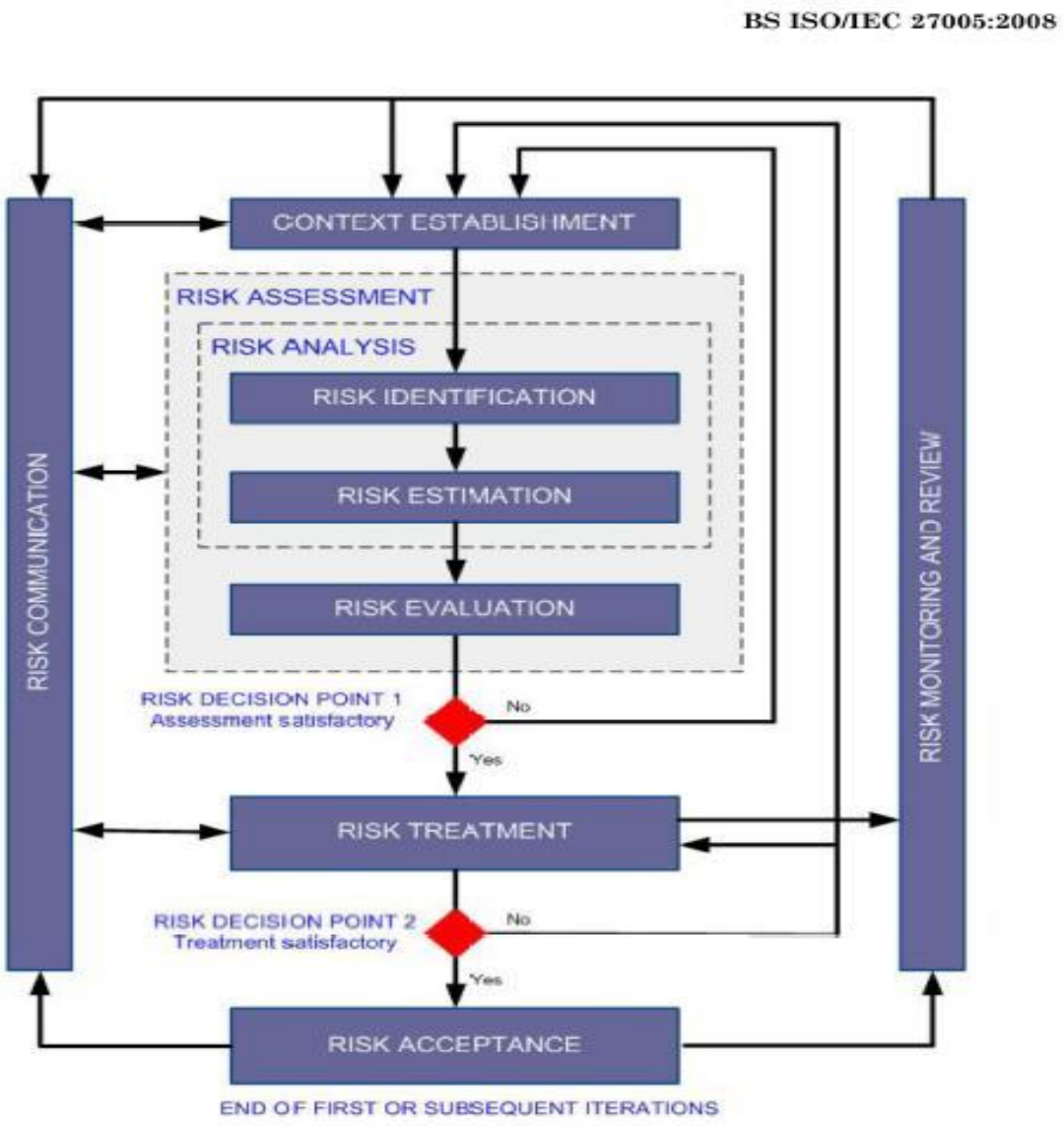
6.3.1 Chấp nhận rủi ro (Risk Acceptance)(2)

- Doanh nghiệp có thể chỉ định một mức chấp nhận rủi ro để dùng tham chiếu khi đánh giá từng rủi ro cụ thể.
- Không một hành động khắc phục nào được thực hiện để tác động đến Khả năng xảy ra và Mức độ ảnh hưởng của rủi ro.

  (Trong ngữ cảnh ATTT, một số tài liệu gọi chấp nhận rủi ro là Giữ lại rủi ro ('Risk Retention') trong khi Chấp nhận rủi ro ('Risk Acceptance') là hành động phê duyệt của cấp có thẩm quyền sau khi kết thúc quá trình QLRR.)

6.3.1 Chấp nhận rủi ro (Risk Acceptance)(3)

- Trong ngữ cảnh QLRR ATTT theo tiêu chuẩn ISO 27005:2008, Chấp nhận rủi ro ('Risk Acceptance') là hành động phê duyệt các chiến lược và giải pháp xử lý rủi ro của cấp có thẩm quyền vào cuối quá trình QLRR.



6.3.1 Chấp nhận rủi ro (Risk Acceptance)(4)

- Tại sao doanh nghiệp chọn chiến lược chấp nhận rủi ro?

  Lý do phổ biến nhất là chi phí của các chiến lược QLRR khác, như phòng ngừa hoặc hạn chế rủi ro, có thể lớn hơn chi phí của chính rủi ro đó. Doanh nghiệp có lợi ích gì khi chi 10.000 USD để tránh rủi ro 1.000 USD?

- Chấp nhận rủi ro là lựa chọn ít tốn kém nhất trong thời gian ngắn và nhưng thường là lựa chọn tốn kém nhất trong dài hạn nếu một sự kiện tiêu cực xảy ra (ví dụ sự cố xảy ra gây gián đoạn vận hành mạng).

6.3.1 Chấp nhận rủi ro (Risk Acceptance)(5)

Một số ví dụ về việc chọn chiến lược chấp nhận rủi ro trong ATTT:

- Duy trì hoạt động của hệ điều hành cũ (MS Windows 98/XP/…) nếu các máy tính dùng hệ điều hành đó không được kết nối với môi trường dữ liệu nhạy cảm.
- Cho phép nhân viên kết nối thiết bị di động riêng của họ với mạng của doanh nghiệp nếu thiết bị này truy cập vào dữ liệu lưu trữ trong các mạng không có thông tin nhạy cảm và mạng đã được phân tách (segmentation).

6.3.2 Giảm nhẹ rủi ro (Risk Mitigation)[1]

- Giảm nhẹ rủi ro là một chiến lược nhằm chuẩn bị và giảm thiểu tác động của các mối đe dọa mà doanh nghiệp phải đối mặt
- Hành động được thực hiện để giảm thiểu khả năng xảy ra ('likelihood') hoặc mức độ ảnh hưởng ('impact') của rủi ro, hoặc giảm thiểu cả hai.

6.3.2 Giảm nhẹ rủi ro (Risk Mitigation)(2)

Một số ví dụ về việc chọn chiến lược giảm nhẹ rủi ro ATTT:

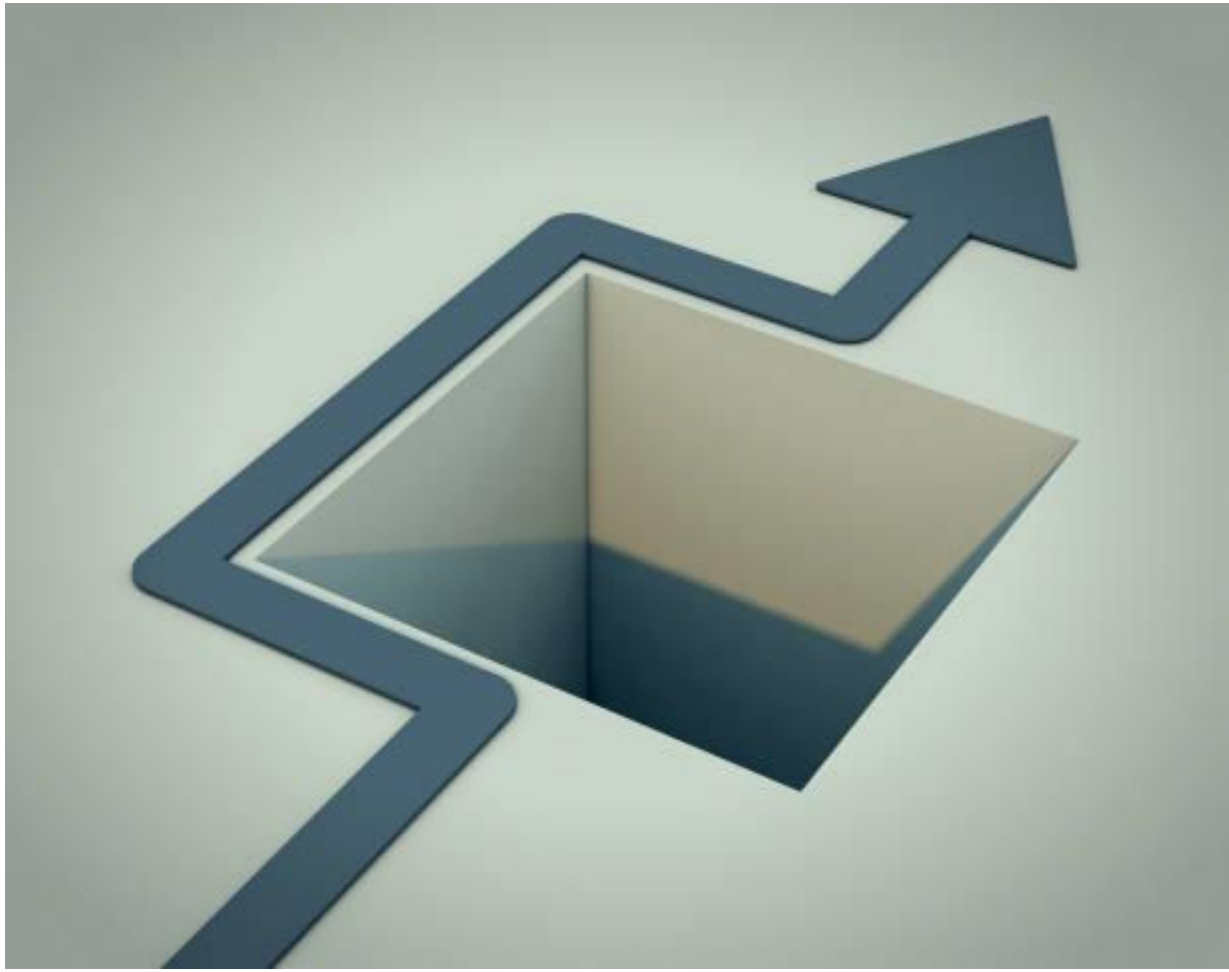
- Đào tạo nâng cao nhận thức ATTT cho người lao động;
- Xác thực 2 yếu tố khi chứng thực giao dịch thanh toán.
- Xác thực 2 lớp khi truy cập vật lý (số PIN kết hợp thẻ ra vào) ra vào phòng làm việc.
- Cài đặt tường lửa là chiến lược giảm nhẹ rủi ro để chặn vi-rút máy tính và các kẻ xâm nhập mạng không đáng tin cậy truy cập vào mạng doanh nghiệp.

6.3.3 Tránh né rủi ro (Risk Avoidance) (1)

- Tránh né rủi ro là việc loại bỏ các mối nguy hiểm, các hoạt động và sự phơi bày (nhiễm) có thể ảnh hưởng tiêu cực đến doanh nghiệp và tài sản của doanh nghiệp.

6.3.3 Tránh né rủi ro (Risk Avoidance)(2)

- Tránh né rủi ro tìm cách tránh hoàn toàn các sự kiện gây tổn hại cho tài sản hay cho doanh nghiệp; tránh các hoạt động tạo nên rủi ro, không tiến hành công việc có rủi ro hoặc lựa chọn phương án thay thế để không gặp rủi ro.



6.3.3 Tránh né rủi ro (Risk Avoidance) (3)

Một số ví dụ về việc chọn chiến lược tránh né rủi ro ATTT:

- Loại bỏ các ứng dụng cũ (legacy); xác thực không mật khẩu; mã hóa dữ liệu nhạy cảm với độ dài khóa 265 bit hoặc cao hơn v.v.
- Loại bỏ quyền truy cập đặc quyền vô thời hạn;
- Hoạch định kinh doanh liên tục có chiều sâu;
- Phân tích rủi ro trước khi mua sản phẩm, dịch vụ của bên thứ ba;
- v.v.

6.3.4 Chuyển giao rủi ro (Risk Transfer)(1)

- Chuyển giao rủi ro là một chiến lược QLRR bao gồm việc chuyển giao rủi ro thuần túy (một phần hoặc toàn bộ) theo hợp đồng từ bên này sang bên khác; giao trách nhiệm xử lý sự kiện rủi ro và tác động của rủi ro cho bên tiếp nhận.

6.3.4 Chuyển giao rủi ro (Risk Transfer) (2)

Các phương thức chuyển giao rủi ro bao gồm:

1. Bảo hiểm (‘Insurance’);
2. Hợp đồng có điều khoản bồi thường (‘Contracts with an Indemnification Clause’); và
3. Thuê dịch vụ của bên thứ ba (‘Outsourcing’).

6.3.4 Chuyển giao rủi ro (Risk Transfer) (3)

1. Bảo hiểm (Insurance):

- Doanh nghiệp có thể mua hợp đồng bảo hiểm từ công ty bảo hiểm và tự bảo vệ mình khỏi những tác động của rủi ro trong tương lai.
- Trong trường hợp có hợp đồng bảo hiểm, bên bảo hiểm (hay Người bồi thường) sẽ bảo vệ chủ hợp đồng (hoặc người được bảo hiểm hay người được bồi thường) khỏi các tình huống bất ngờ trong tương lai.

6.3.4 Chuyển giao rủi ro (Risk Transfer)(4)

2. Hợp đồng có điều khoản bồi thường (‘Contracts with an Indemnification Clause’):

Doanh nghiệp sử dụng hợp đồng có điều khoản bồi thường để chuyển giao rủi ro.

https://www.typecalendar.com/indemnity-agreement.html

6.3.4 Chuyển giao rủi ro (Risk Transfer) (5)

2. Hợp đồng có điều khoản bồi thường ('Contracts with an Indemnification Clause'):

(…) Các hợp đồng có điều khoản như vậy đảm bảo việc chuyển rủi ro tài chính từ người được bồi thường (là doanh nghiệp) sang người bồi thường. Trong thỏa thuận như vậy, những tổn thất trong tương lai của người được bồi thường sẽ do người bồi thường chịu.

6.3.4 Chuyển giao rủi ro (Risk Transfer)(6)

3. Thuê dịch vụ của bên thứ ba (Outsourcing):

- Thuê bên thứ ba (như thuê gia công phần mềm) cung cấp dịch vụ cho doanh nghiệp là một hình thức chuyển giao rủi ro trong đó một quy trình hoặc dự án được thuê ngoài để chuyển các rủi ro khác nhau từ bên này sang bên khác.
- Doanh nghiệp muốn tập trung vào hoạt động kinh doanh cốt lõi của mình, doanh nghiệp có thể thuê bên thứ ba làm các hoạt động phụ trợ cho mình thay vì tự làm.

6.3.4 Chuyển giao rủi ro (Risk Transfer)(7)

Một số ví dụ về việc chọn chiến lược chuyển giao rủi ro ATTT:

- Thuê công ty IBM quản lý dịch vụ CNTT cho doanh nghiệp (như dịch vụ bảo trì phần cứng (máy chủ…), phát triển trang Web…);
- Thuê công ty FPT gia công phần mềm;
- Thuê công ty CMC cung cấp dịch vụ HelpDesk, an toàn mạng, quản lý trung tâm dữ liệu…;
- v.v.

Hết Chương 6

Cám ơn tất cả Anh/Chị đã theo dõi Chương này

(*)Một số hình minh họa được tải từ trang https://www.pexels.com/ và https://pixabay.com/