QUẢN LÝ AN TOÀN THÔNG TIN

QUẢN LÝ RỦI RO:
XÁC ĐỊNH VÀ ĐÁNH GIÁ RỦI RO

CÂU CHUYỆN THỰC TẾ

Một công ty bị thua lỗ nặng nề chỉ trong một đêm khi văn phòng của họ bị cháy rụi.
Khi các nhân viên tập trung quanh những gì còn sót lại vào sáng hôm sau, giám đốc hỏi thư ký cô ấy đã thực hiện sao lưu máy tính hàng ngày chưa. Ông cảm thấy nhẹ nhõm khi cô trả lời là có. Mỗi ngày trước khi về nhà cô đều sao lưu tất cả các thông tin tài chính, hóa đơn, đơn đặt hàng ...
Giám đốc sau đó yêu cầu thư ký lấy lại bản sao lưu để họ có thể bắt đầu xác định tình trạng tài chính hiện tại của mình.
“Chà”, cô thư ký nói, “Tôi đoán là tôi không thể. Ông thấy đấy, tôi đã để những bản sao lưu đó trong ngăn bàn bên cạnh máy tính trong văn phòng. ”

Management of Information Security, 3rd ed.

NỘI DUNG

I. GIỚI THIỆU
II. QUẢN LÝ RỦI RO
III. NHẬN DẠNG RỦI RO
IV. ĐÁNH GIÁ RỦI RO
V. VIẾT BÁO CÁO KẾT QUẢ ĐÁNH GIÁ RỦI RO
VI. TÓM TẮT CHƯƠNG

MỤC TIÊU CẦN ĐẠT

- Định nghĩa và vai trò quản lý rủi ro trong tổ chức
- Các kỹ thuật quản lý rủi ro để xác định và xếp hạng các yếu tố rủi ro đối với tài sản thông tin.
- Giải thích cách đánh giá rủi ro dựa trên khả năng xảy ra các sự kiện gây bất lợi và ảnh hưởng đến tài sản thông tin khi các sự kiện này xảy ra.
- Thảo luận về việc sử dụng các kết quả của quá trình xác định rủi ro.

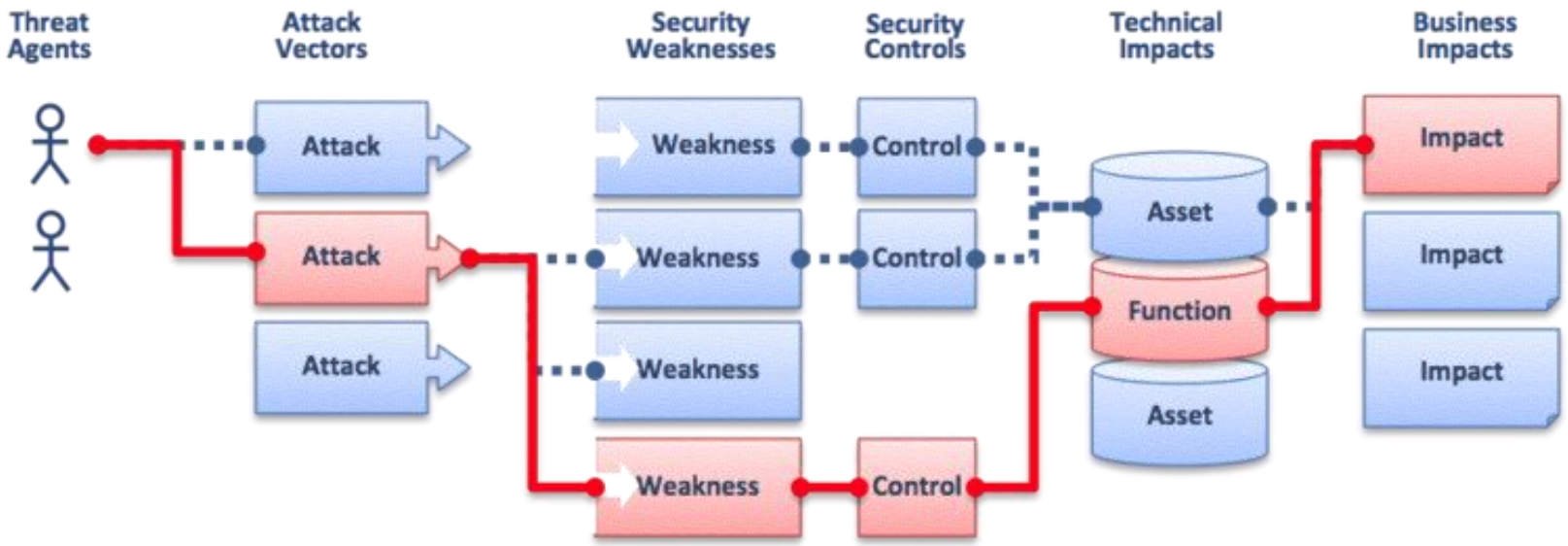
I. GIỚI THIỆU

Quản lý rủi ro:

- Là quá trình:
  - Xác định mức rủi ro tổng thể tối đa có thể chấp nhận
  - Sử dụng các kỹ thuật đánh giá rủi ro để xác định mức rủi ro
  - Phát triển một chiến lược để cải thiện các rủi ro riêng lẻ thích hợp để mức rủi ro tổng thể xuống mức có thể chấp nhận.
- Là một trong những trách nhiệm chính của các quản lý trong tổ chức
- Hai quy trình chính:
  - Xác định và đánh giá rủi ro
  - Kiểm soát rủi ro

I. GIỚI THIỆU
Các thuật ngữ liên quan đến rủi ro

I. GIỚI THIỆU
Các thuật ngữ liên quan đến rủi ro



I. GIỚI THIỆU

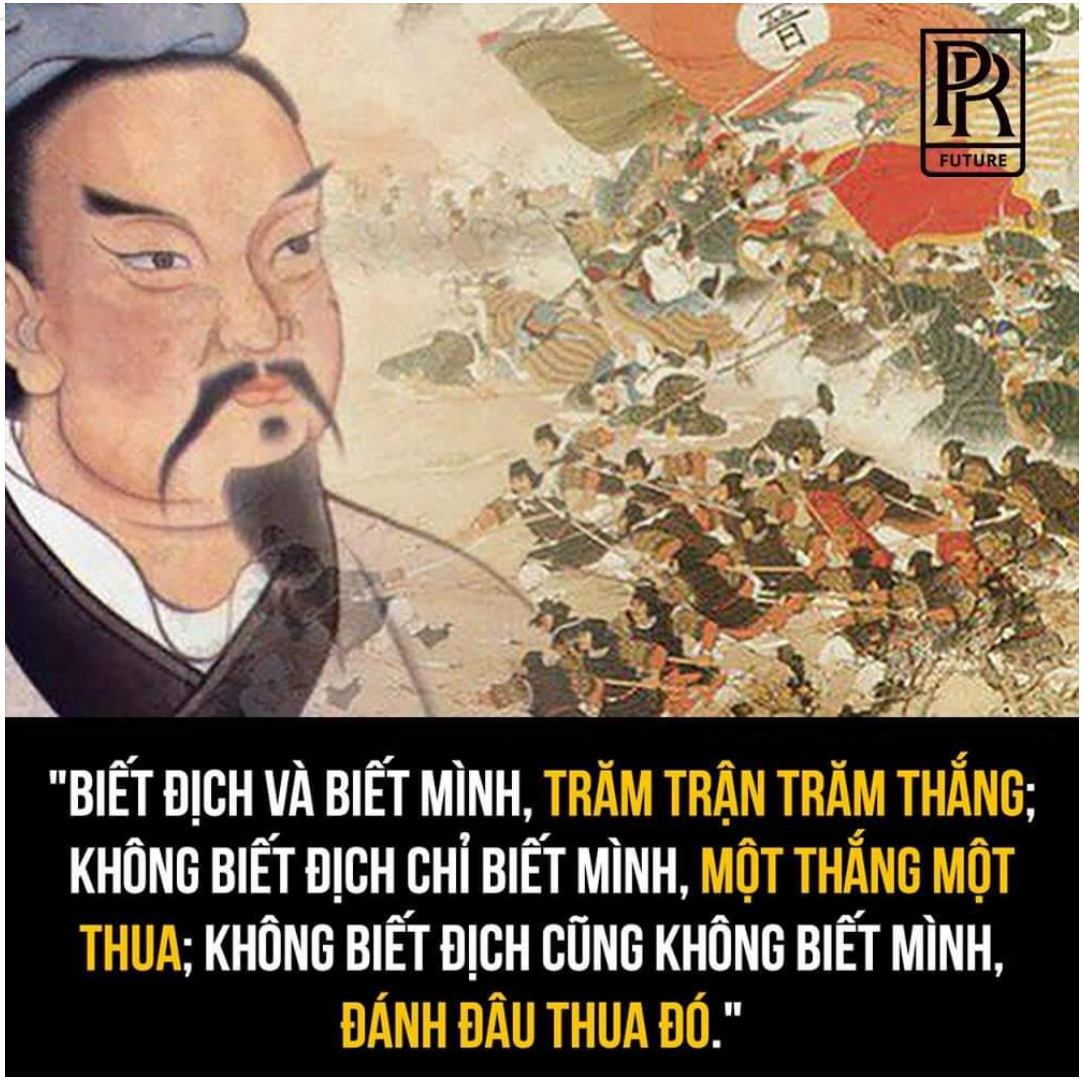
- An toàn thông tin (Information Security - InfoSec) trong một tổ chức tồn tại chủ yếu để quản lý rủi ro CNTT.
- Quản lý rủi ro là một trong những trách nhiệm chính của mọi nhà quản lý trong tổ chức.
- Mỗi nhà quản lý trong tổ chức nên tập trung vào việc giảm thiểu rủi ro. Điều này thường được thực hiện trong sự phối hợp của ba đối tượng, cụ thể như sau:

I. GIỚI THIỆU

3 nhóm quản lý:

- Ban quản lý chung phải cấu trúc các chức năng CNTT và InfoSec bảo vệ thành công tài sản thông tin của tổ chức.
- Quản lý CNTT phải phục vụ nhu cầu CNTT rộng hơn, khai thác các kỹ năng và hiểu biết đặc biệt của cộng đồng InfoSec(ATTT).
- Quản lý ATTT phải dẫn đầu với kỹ năng, tính chuyên nghiệp và tính linh hoạt vì nó hoạt động với nhóm quản lý khác để cân bằng giữa tính hữu dụng và bảo mật.

II. QUẢN LÝ RỦI RO



“ Chiến lược và chiến thuật InfoSec theo nhiều cách tương tự như những chiến thuật được sử dụng trong chiến tranh thông thường “

II. QUẢN LÝ RỦI RO

1. Biết ta

- Tổ chức nào cũng có một lượng rủi ro nhất định.
- Luôn phải hiểu cách thông tin được xử lý, lưu trữ và truyền tải, tài sản nào có giá trị.
- Quản lý rủi ro là một quá trình.

2. Biết người

- Xác định, kiểm tra và hiểu các mối đe dọa
- Quản lý rủi ro là quá trình phát hiện, đánh giá rủi ro và xác định cách thức kiểm soát, giảm thiểu.
- Phân tích rủi ro là việc xác định và đánh giá các mức độ rủi ro.

II. QUẢN LÝ RỦI RO

3. Trách nhiệm giải trình đối với quản lý rủi ro

- Tất cả các cộng đồng quan tâm đều chịu trách nhiệm về việc quản lý rủi ro :

- InfoSec —lãnh đạo trong việc giải quyết rủi ro.
- IT —giúp xây dựng các hệ thống an toàn và đảm bảo hoạt động của chúng.
- Quản lý và người dùng —phát hiện và phản hồi sớm. đảm bảo đủ nguồn lực phân bổ cho InfoSec và IT

II. QUẢN LÝ RỦI RO

3. Trách nhiệm giải trình đối với quản lý rủi ro

- Thực hiện các hoạt động sau:
  - Đánh giá các biện pháp kiểm soát rủi ro.
  - Xác định các tùy chọn kiểm soát với chi phí phù hợp.
  - Mua hoặc cài đặt các điều khiển thích hợp.
  - Giám sát các quy trình để đảm bảo các biện pháp kiểm soát vẫn hiệu quả.
  - Xác định các rủi ro
  - Đánh giá rủi ro
  - Tóm tắt các kết quả

III. Nhận dạng rủi ro

Lập kế hoạch và tổ chức quy trình
Tạo danh mục thành phần hệ thống
Triển khai danh sách kiểm kê tài sản
Xác định các mối đe dọa
Xác định tài sản dễ bị tấn công
Chỉ định giá trị hoặc đánh giá tác động tới tài sản
Đánh giá khả năng xảy ra đối với các lỗ hổng
Tính hệ số rủi ro tương đối cho tài sản
Đánh giá sơ bộ các biện pháp kiểm soát có thể có
Tìm kiếm tài liệu

Quy trình xác định và đánh giá rủi ro

III. Nhận dạng rủi ro
1. Tạo kho tài sản thông tin

Thành phần hệ thống CNTT	Các thành phần quản lý rủi ro	Ví dụ về thành phần Quản lý Rủi ro
Con người	Nhân sự nội bộ Nhân viên bên ngoài	-Nhân viên đáng tin cậy -Các nhân viên khác -Những người chúng tôi tintưởng bên ngoài tổ chức của chúng tôi -Người lạ
Quy Trình	Quy trình liên quan	+Các quy trình tiêu chuẩn kinh doanh và CNTT +Các quy trình nhạy cảm về CNTT và kinh doanh
Dữ liệu	Dữ liệu/Thông tin	+ Quá trình vận chuyển +Xử lý dữ liệu + Kho lưu trữ
Phần mềm	Phần mềm	+Các ứng dụng +Các hệ điều hành +Thành phần bảo mật
Phần cứng	Phần cứng	+Hệ thống và thiết bị ngoại vi +Thiết bị an ninh
Kết nối mạng	Kết nối mạng	+Các thành phần mạng cục bộ +Các thành phần mạng nội bộ +Các thành phần Internet hoặc extranet +Các thành phần dựa trên đám mây

Tài sản của tổ chức được sử dụng trong hệ thống

III. Nhận dạng rủi ro
1. Tạo kho tài sản thông tin

- Mô hình đơn giản:

Con người, **Quy trình** và **Công nghệ** (PPT).

- **Xác định Tài sản Phần cứng, Phần mềm và Mạng** :
- Cần số lượng kế hoạch nhất định.
- Xác định thuộc tính nào được theo dõi:Tên , thẻ tài sản (asset tag), IP, MAC, loại tài sản,…
- **Xác định Con người, Quy trình và Tài sản Dữ liệu**
- Khó xác định và ghi lại
- Giao cho các quản lý có kiến thức, kinh nghiệm.
- Ghi lại qua: Quy trình xử lý dữ liệu tin cậy. Hệ thống lưu trữ linh hoạt, cho phép liên kết nội dung với các thuộc tính.

III. Nhận dạng rủi ro
1. Tạo kho tài sản thông tin

- Các thuộc tính cơ bản:

- Con người:

Tên / số / ID chức vụ ; Tên / số / ID người giám sát;…

- Quy Trình:

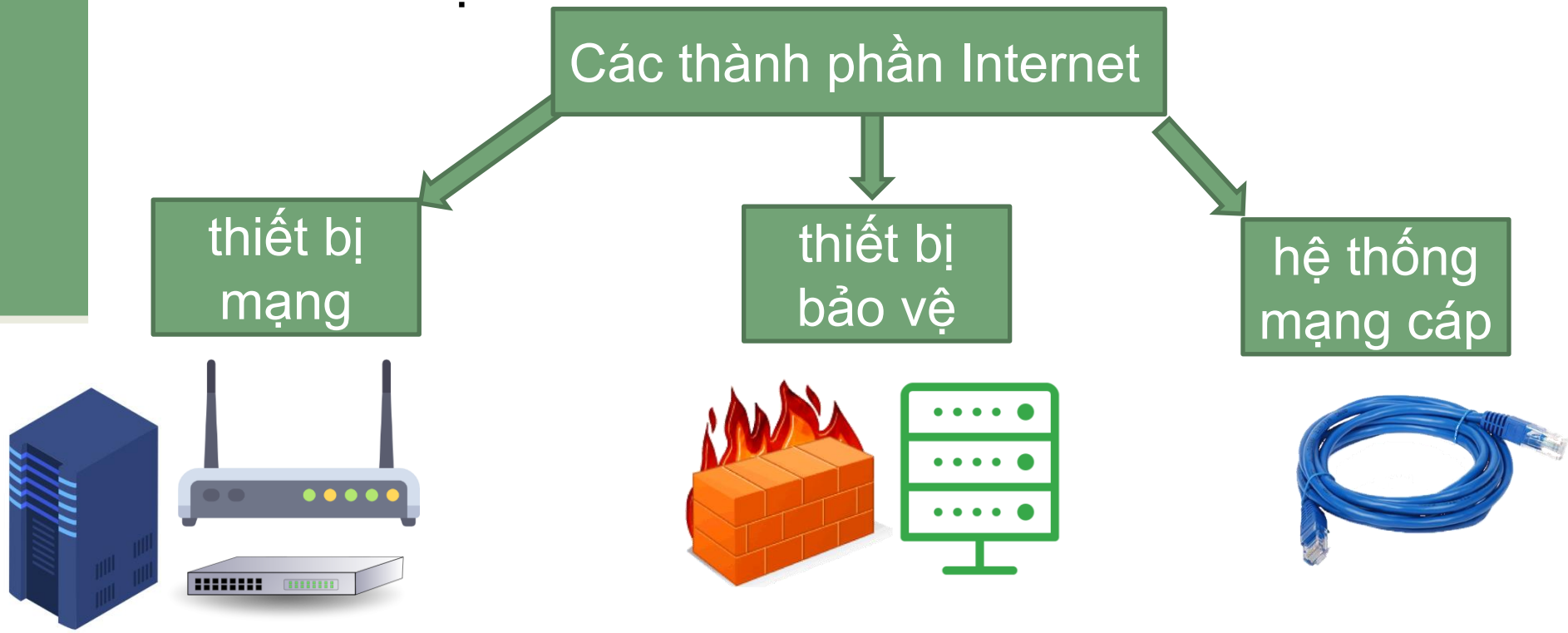
Mô tả; Mục đích dự định; Phần mềm / phần cứng / phần tử mạng mà quy trình được ràng buộc với nhau,...

- Dữ liệu:

Phân loại; Chủ sở hữu / người sáng tạo / người quản lý; Kích thước của cấu trúc dữ liệu;...

III. Nhận dạng rủi ro
2. Phân loại và mức độ của tài sản

- Xác định ý nghĩa tài sản đối với chương trình quản lý rủi ro. chia nhỏ hơn nữa các danh mục được trình bày trong Bảng Tài sản của tổ chức được sử dụng trong hệ thống hoặc tạo ra các danh mục mới.



III. Nhận dạng rủi ro
2. Phân loại và mức độ của tài sản

- Tạo danh sách phân bố mức độ nhạy cảm và mức độ ưu tiên bảo mật được chỉ định cho từng tài sản. Mỗi danh mục chỉ định mức độ bảo vệ cần thiết cho một tài sản thông tin cụ thể.
- Các danh mục phân loại phải toàn diện, loại trừ lẫn nhau
- “Toàn diện” : tất cả các tài sản được kiểm kê đều phù hợp với một danh mục;
- "Loại trừ lẫn nhau" :mỗi nội dung chỉ được tìm thấy trong một danh mục.

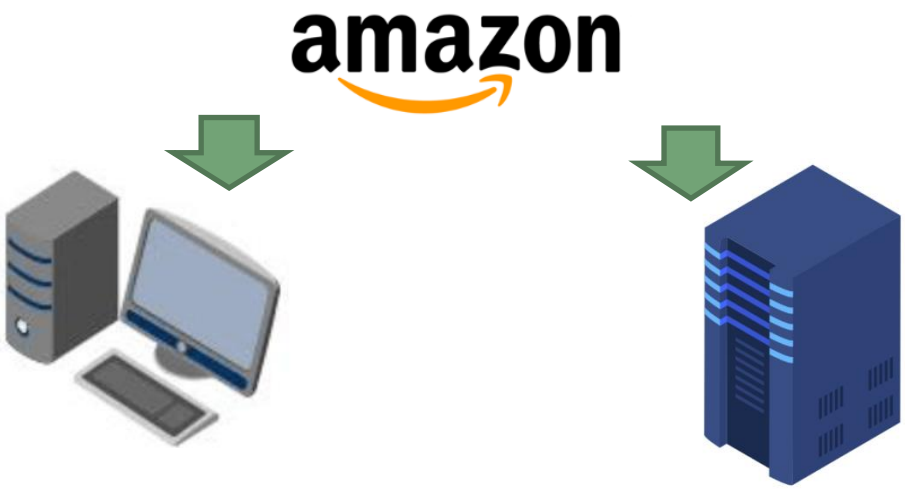
III. Nhận dạng rủi ro
3. Đánh giá giá trị cho tài sản thông tin

- Đánh giá tương đối: đảm bảo rằng các tài sản có giá trị cao hơn được bảo vệ trước.
- Trả lời các câu hỏi:
- *Tài sản thông tin nào là quan trọng nhất đối với sự thành công của tổ chức?*
- *Tài sản thông tin nào tạo ra nhiều doanh thu nhất?*
- *Tài sản thông tin nào tạo ra khả năng sinh lời cao nhất?*

....

III. Nhận dạng rủi ro
3. Đánh giá giá trị cho tài sản thông tin

Ví dụ: *Xếp hạng tài sản của Amazon:*



Tại Amazon.com:

- *Các máy chủ hỗ trợ bán sách (mang lại doanh thu cao nhất)*
- *Các máy chủ khác hỗ trợ bán các sản phẩm làm đẹp (mang lại lợi nhuận cao nhất).*

III. Nhận dạng rủi ro
3. Đánh giá giá trị cho tài sản thông tin

Tên hệ thống: SLS E-Commerce Ngày đánh giá: 02/2008 Đánh giá bởi: D.Jones		
Tài sản thông tin	Phân loại dữ liệu	Tác động đến lợi nhuận
<u>Thông tin được truyền đi:</u>		
Bộ tài liệu EDI 1 – Vận đơn hậu cần cho người thuê ngoài (xuất khẩu)	Bí mật	Cao
Bộ tài liệu EDI 2 – Nhà cung cấp đặt hàng (xuất khẩu)	Bí mật	Cao
Bộ tài liệu EDI 2 – Ý kiến về dịch vụ hoàn tất đơn hàng từ nhà cung cấp (trong nước)	Bí mật	Trung bình
Khách hàng đặt hàng qua SSL (trong nước)	Bí mật	Nghiêm trọng
Dịch vụ khách hàng yêu cầu qua e-mail (trong nước)	Riêng tư	Trung bình

Bảng 3. Sơ đồ phân loại tài sản mẫu

III. Nhận dạng rủi ro
3. Đánh giá giá trị cho tài sản thông tin

Tên hệ thống: SLS E-Commerce Ngày đánh giá: 02/2008 Đánh giá bởi: D.Jones		
<u>Tài sản DMZ:</u>		
Bộ định tuyến cạnh	Công khai	Nghiêm trọng
Máy chủ Web #1 – Trang chủ và trang chính	Công khai	Nghiêm trọng
Máy chủ Web #2 – Máy chủ ứng dụng	Riêng tư	Nghiêm trọng
Chú thích: BOL: Bill of Lading – Vận đơn DMZ: Demilitarized Zone – Khu phi quân sự EDI: Electronic Data Interchange – Trao đổi dữ liệu điện tử SSL: Secure Socket Layer – Giao thức bảo mật		

Bảng 3. Sơ đồ phân loại tài sản mẫu

III. Nhận dạng rủi ro

4. Liệt kê tài sản theo thứ tự quan trọng

Tài sản thông tin	Tiêu chí 1: Ảnh hưởng đến doanh thu	Tiêu chí 2: Ảnh hưởng đến khả năng sinh lời	Tiêu chí 3: Ảnh hưởng đến hình ảnh công chúng	Điểm số
Trọng số đánh giá (1 - 100); phải tổng 100	30	40	30	
Bộ tài liệu EDI 1 - Vận đơn hậu cầu cho người thuê ngoài (xuất khẩu)	0.8	0.9	0.5	75
Bộ tài liệu EDI 2 - Nhà cung cấp đơn đặt hàng (nước ngoài)	0.8	0.9	0.6	78
Bộ tài liệu EDI 2 — Tư vấn đáp ứng của nhà cung cấp (trong nước)	0.4	0.5	0.3	41
Khách hàng đặt hàng qua SSL (trong nước)	1	1	1	100
Yêu cầu dịch vụ khách hàng qua e-mail (trong nước)	0.4	0.4	0.9	55

Ví dụ về bảng phân tích nhân tố có trọng số

III. Nhận dạng rủi ro
5. Nhận dạng mối đe dọa

- **Xác định và Ưu tiên các Đe doạ và Tác nhân Đe doạ**

Đặt những câu hỏi để hiểu về chúng, tác động tiềm ẩn của chúng đối với tài sản thông tin:

- *Những mối đe dọa nào gây nguy hiểm cho tài sản thông tin của tổ chức này trong môi trường hiện tại?*
- *Những mối đe dọa nào gây nguy hiểm cho tài sản thông tin của tổ chức này trong môi trường hiện tại?*

III. Nhận dạng rủi ro
5. Nhận dạng mối đe dọa

Mối đe dọa	Ví dụ
Thỏa hiệp với sở hữu trí tuệ	Vi phạm bản quyền phần mềm hoặc vi phạm bản quyền khác
Chênh lệch về chất lượng dịch vụ từ các nhà cung cấp dịch vụ	Biến động về nguồn điện, dữ liệu và các dịch vụ khác
Gián điệp hoặc xâm phạm	Truy cập trái phép và / hoặc thu thập dữ liệu
Thảm họa tự nhiên	Cháy, lũ lụt, động đất, sét, v.v.
Lỗi do con người	Tai nạn, sai lầm của nhân viên, không tuân thủ chính sách
Tống tiền thông tin	Đe dọa tống tiền tiết lộ thông tin
Phá hoại	Gây hư hỏng hoặc phá hủy hệ thống hoặc thông tin
Phần mềm độc hại	vi rút, sâu, macro, từ chối dịch vụ hoặc script injections
Lỗi kỹ thuật về phần cứng	Lỗi thiết bị phần cứng
Lỗi kỹ thuật về phần mềm	Lỗi, sự cố mã, sơ hở, cửa hậu
Công nghệ lỗi thời	Các công nghệ cổ hủ hoặc lạc hậu
Trộm	Tịch thu bất hợp pháp thiết bị hoặc thông tin

Các mối đe dọa đối với InfoSec

III. Nhận dạng rủi ro
5. Nhận dạng mối đe dọa

- **Tần suất các cuộc tấn công**

- Số lượng cuộc tấn công được phát hiện **Giảm**
- Số lượng báo cáo tấn công phần mềm độc hại **Tăng**.
- Số tổ chức báo cáo số lượng, chi phí của các cuộc tấn công thành công cũng đang **Giảm**
- Đặt các câu hỏi cơ bản:

- *Sẽ tốn bao nhiêu để phục hồi sau một cuộc tấn công thành công?*
- *Những mối đe dọa nào đòi hỏi chi phí lớn nhất để ngăn chặn?*

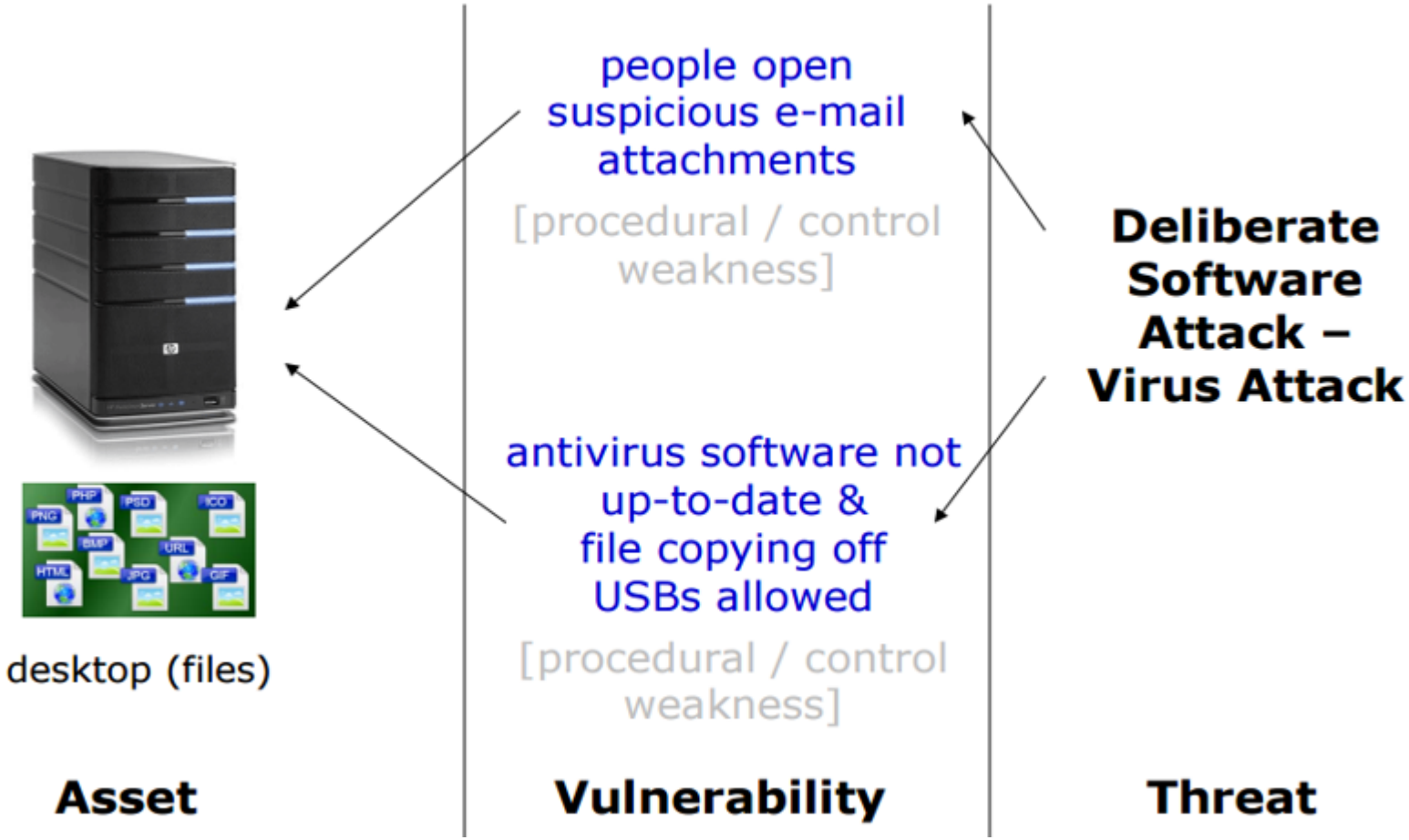
III. Nhận dạng rủi ro
6. Các phương pháp đánh giá các mối đe doạ

Câu trả lời	Phần trăm lựa chọn
Xác suất xảy ra	85.4%
Khủng hoảng truyền thông	77.1%
Thua lỗ	72.9%
Chi phí phòng chống các mối đe doạ	64.6%
Chi phí khắc phục sau khi bị tấn công	64.6%
Tần suất các cuộc tấn công	52.1%
Mất lợi thế cạnh tranh	35.4%
Câu trả lời khác	6.3%

Đánh giá các mối đe doạ cơ bản

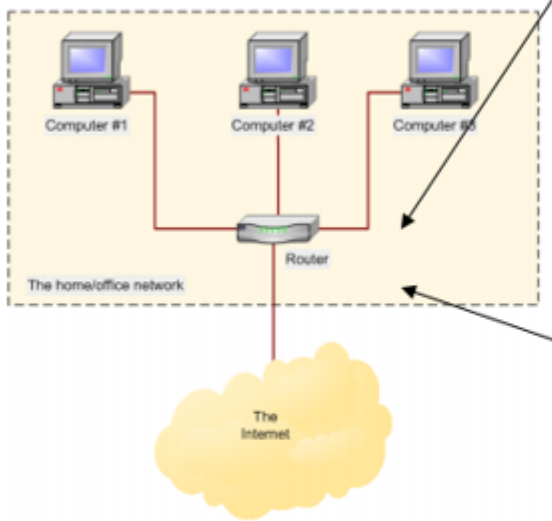
III. Nhận dạng rủi ro
6. Các phương pháp đánh giá các mối đe doạ

Ví dụ: Đánh giá điểm yếu với tập tin quan trọng



III. Nhận dạng rủi ro
6. Các phương pháp đánh giá các mối đe doạ

Ví dụ: Đánh giá điểm yếu với bộ định tuyến



router

Asset

temperature control in router/server room is not adequate ⇒ router overheats and shuts downs

[control weakness, design flaw]

net. administrator allows access to unauthor. user ⇒ unauthor. user uploads a virus, router crashes

[control / procedural weakness]

Vulnerability

Act of Human Error or Failure

Threat

III. Nhận dạng rủi ro

6. Các phương pháp đánh giá các mối đe doạ

- **Chi phí cho các mối đe doạ đối với an toàn thông tin:**

Mối đe doạ (Dựa trên ngân sách và nỗ lực để phòng chống và đối phó)	Điểm trung bình 2012	Xếp hạng 2012	Xếp hạng 2003 CACM
Gián điệp hoặc xâm nhập trái phép	4.07	1	6
Tấn công vào phần mềm	3.94	2	1
Trộm cắp	3.18	3	7
Giam chất lượng dịch vụ của nhà cung cấp dịch vụ	3.10	4	5
Thiên tai tự nhiên	3.06	5	10
Phá hoại	3.00	6	8
Công nghệ lỗi thời	2.99	7	9
Lỗi phần mềm	2.71	8	3
Lỗi phần cứng	2.64	9	4
Xâm phạm tài sản trí tuệ	2.55	10	11
Lỗi do con người	2.25	11	2
Tống tiền thông tin	2.00	12	12

Bảng xếp hạng chi phí cho những mối đe doạ hàng đầu

III. Nhận dạng rủi ro
6. Các phương pháp đánh giá các mối đe doạ

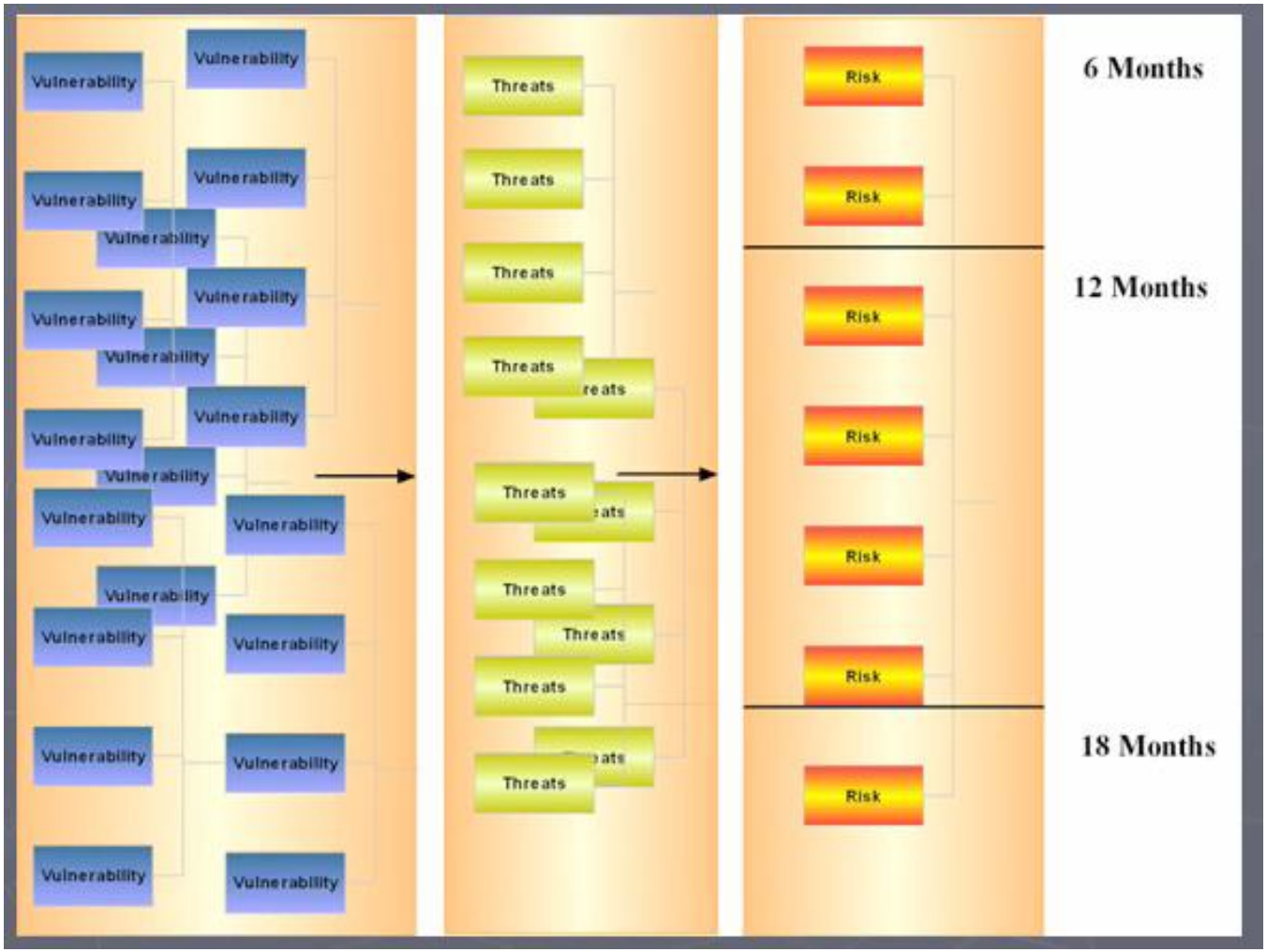
Mối đe doạ	Các điểm yếu tiềm tàng
Xâm phạm tài sản trí tuệ	Bộ định tuyến có ít giá trị nội tại, nhưng các tài sản khác được bảo vệ bởi bộ định tuyến có thể bị tấn công nếu bộ định tuyến bị xâm phạm
Gián điệp hoặc xâm nhập trái phép	Bộ định tuyến có ít giá trị nội tại, nhưng các tài sản khác được bảo vệ bởi bộ định tuyến có thể bị tấn công nếu bộ định tuyến bị xâm phạm
Thiên tai tự nhiên	Tất cả các tài sản thông tin trong tổ chức là mục tiêu của thiên tai tự nhiên trừ khi các biện pháp kiểm soát phù hợp được đưa ra
Lỗi do con người	Nhân viên hoặc nhà thầu có thể gây ra sự cố nếu có lỗi cấu hình
Tống tiền thông tin	Bộ định tuyến có ít giá trị nội tại, nhưng các tài sản khác được bảo vệ bởi bộ định tuyến có thể bị tấn công nếu bộ định tuyến bị xâm phạm
Giảm chất lượng dịch vụ của nhà cung cấp dịch vụ	Trừ khi được cung cấp nguồn điện phù hợp, hiện tượng sập nguồn rất dễ xảy ra theo thời gian
Phá hoại	IP dễ bị tấn công từ chối dịch vụ. Thiết bị có thể bị phá hoại hoặc làm hư hại bộ nhớ cache

III. Nhận dạng rủi ro
6. Các phương pháp đánh giá các mối đe doạ

Tấn công phần mềm	IP dễ bị tấn công từ chối dịch vụ. Các hoạt động lấy dấu vân tay IP của người ngoài có thể tiết lộ các thông tin nhạy cảm trừ khi các biện pháp kiểm soát phù hợp được thực hiện
Lỗi phần cứng	Phần cứng có thể bị lỗi và gây ra sự cố Sự cố hệ thống điện luôn có thể xảy ra
Lỗi phần mềm	Phần mềm định tuyến do nhà cung cấp cung cấp có thể bị lỗi và gây mất điện
Công nghệ lỗi thời	Nếu công nghệ không được xem xét và cập nhật định kỳ, một thiết bị có thể tụt hậu quá xa so với mô hình mà nhà cung cấp của nó hỗ trợ để được duy trì dịch vụ
Trộm cắp	Bộ định tuyến có ít giá trị nội tại, nhưng các tài sản khác được bảo vệ bởi bộ định tuyến có thể bị tấn công nếu bộ định tuyến bị xâm phạm

Đánh giá điểm yếu của DMZ router

III. Nhận dạng rủi ro
6. Các phương pháp đánh giá các mối đe doạ



III. Nhận dạng rủi ro
7. Bảng TVA

Danh sách tài nguyên và các điểm yếu theo thứ tự ưu tiên
Danh sách mối đe doạ theo thứ tự ưu tiên có trọng số
➔ Bảng TVA (Threats-Vulnerabilities-Assets)

	Asset 1	Asset 2	…	…	…	…	…	…	…	…	…	Asset n
Threat 1												
Threat 2												
…												
…												
…												
…												
…												
…												
…												
…												
Threat n												
Độ kiểm soát ưu tiên	1		2		3		4		5		6	
Các dải kiểm soát này cần được tiếp tục thông qua tất cả các cặp asset-threat												

Bảng TVA mẫu

IV. ĐÁNH GIÁ RỦI RO

Việc đánh giá rủi ro tương đối cho mỗi lỗ hổng được thực hiện thông qua một quá trình được gọi là **đánh giá rủi ro (risk assessment)**.

IV. ĐÁNH GIÁ RỦI RO
1. Mục tiêu của việc đánh giá rủi ro

- Để tạo ra một phương pháp lặp để đánh giá một cách tương đối các rủi ro đã được phát hiện và thêm vào danh sách. Cho mỗi lỗ hổng một số điểm hoặc một đánh giá rủi ro (Risk Rating).

- Điểm số này giúp đánh giá được rủi ro một cách tương đối cho từng tài sản, là cơ sở cho các phương pháp đánh giá rủi ro chính xác hơn.

IV. ĐÁNH GIÁ RỦI RO
2. Khả năng xảy ra (Likelihood)

- Là một đánh giá tổng hợp – một con số trên một thước đo đã định về khả năng một lỗ hổng xác định để tấn công và khai thác.

- 2 thước đo để đánh giá :
  - NIST : Lổ hổng được cho điểm từ 0.1 (Low) - 1.0 (High)
  - Thước đo rủi ro từ 1 đến 100

- Nên dùng các nguồn thông tin bên ngoài rồi điều chỉnh cho phù hợp trường hợp của mình

IV. ĐÁNH GIÁ RỦI RO
3. Đánh giá những mất mát tiềm tàng

- Sau khi liệt kê được các lỗ hổng , ta gán cho mỗi tài sản thông tin một số điểm rồi tiến hành nghiên cứu đánh giá.

- Điểm được tính bằng cách trả lời các câu hỏi về "Phát hiện và ưu tiên các mối đe dọa và các tác nhân của mối đe dọa" ("Identify and Prioritize Threats and Threat Agents")

- Bước tiếp theo : "Xem xét xem các biện pháp hiện tại chống đỡ lại các mối đe dọa do các lỗ hổng riêng biệt"

IV. ĐÁNH GIÁ RỦI RO

4. Phần trăm các rủi ro được giảm nhẹ bởi các biện pháp hiện tại

Nếu một lỗ hổng được kiểm soát một phần , hãy ước lượng phần trăm lỗ hổng đấy được kiểm soát

5. Độ không chắc chắn

- Không thể biết mọi điều về từng lỗ hổng , các loại tấn công, các tác động của nó lên tổ chức
- Khả năng một biện pháp hiện tại có thể giảm thiểu rủi ro cũng có thể bị ước lượng sai

IV. ĐÁNH GIÁ RỦI RO
6. Xác định rủi ro

Rủi ro là

Khả năng xảy ra của **lỗ hổng**

Nhân với

Giá trị của tài sản thông tin

Trừ đi

Phần trăm rủi ro được giảm thiểu bởi các biện pháp kiểm soát hiện tại

Cộng với

Sự không chắc chắn của kiến thức hiện tại về lỗ hổng bảo mật

IV. ĐÁNH GIÁ RỦI RO
7. Khả năng xảy ra và hậu quả

Cấp độ	Mô tả	Ví dụ của mô tả
1	Không đáng kể	Không chấn thương , tổn thất tài chính nhỏ
2	Nhỏ	Điều trị sơ cứu, các hậu quả giải phóng tại chỗ ngay lập tức được ngăn chặn, tổn thất tài chính trung bình
3	Vừa phải	Cần điều trị y tế, các hậu quả giải phóng tại chỗ với sự hỗ trợ từ bên ngoài, tổn thất tài chính cao
4	Lớn	Tổn thương trên diện rộng, mất khả năng sản xuất, , các hậu quả lan truyền ra bên ngoài mà không ảnh hưởng bất lợi, tổn thất tài chính lớn
5	Thảm khốc	Tử vong, các hậu quả lan truyền ra bên ngoài gây hậu quả bất lợi, tổn thất tài chính lớn

Mức độ thiệt hại đối với các mối đe dọa của tổ chức

IV. ĐÁNH GIÁ RỦI RO
7. Khả năng xảy ra và hậu quả

Cấp độ	Mô tả	Giải thích
A	Gần như chắc chắn	Dự kiến sẽ xảy ra trong hầu hết các trường hợp
B	Rất có thể xảy ra	Có thể sẽ xảy ra trong hầu hết các trường hợp
C	Có thể xảy ra	Có thể xảy ra vào một lúc nào đó
D	Ít khả năng xảy ra	Có thể sẽ xảy ra vào một lúc nào đó
E	Hiếm	Chỉ xảy ra trong các trường hợp hiếm

Mức độ khả năng xảy ra

IV. ĐÁNH GIÁ RỦI RO
7. Khả năng xảy ra và hậu quả

Kết hợp 2 bảng trên ta có:

Cấp độ rủi ro	Hậu quả				
Khả năng xảy ra	Không đáng kể 1	Nhỏ 2	Vừa phải 3	Lớn 4	Thảm khốc 5
A (Gần như chắc chắn)	H	H	E	E	E
B (Rất có thể)	M	H	H	E	E
C (Có thể)	L	M	H	E	E
D (Ít khả năng)	L	L	M	H	E
E (Hiếm)	L	L	M	H	H

Ma trận đánh giá rủi ro định tính

IV. ĐÁNH GIÁ RỦI RO

8. Phát hiện các biện pháp kiểm soát khả thi

- Với các rủi ro dư thừa (Residual Risk) nên có một danh sách sơ bộ về các biện pháp kiểm soát khả thi để phát hiện các nơi có và có cần phải giảm thiểu chúng không.
- “Kiểm soát” , “Bảo vệ” , “Phòng chống” miêu tả các cơ chế , chính sách bảo vệ giúp giảm rủi ro, cải thiện an ninh.

V. ĐÁNH GIÁ RỦI RO

9. Kiểm soát truy cập

- Cần chỉ rõ việc cho một người dùng vào khu vực tin cậy của tổ chức (hệ thống thông tin, phòng máy tính,…)
- Kiểm soát truy cập là một tổ hợp về chính sách , chương trình và công nghệ
- Mỗi loại kiểm soát quy định quyền truy cập đến một loại hoặc tập hợp các thông tin cụ thể.

Đánh giá Rủi ro Định tính

Quá trình đánh giá rủi ro định tính của một cuộc tấn công

Ví dụ về Đánh giá Rủi ro Định tính

Mối nguy hại	Ảnh hưởng	Xác suất xảy ra (khi chưa áp dụng các biện pháp phòng ngừa)	Biện pháp phòng ngừa	Xác suất xảy ra (khi đã áp dụng các biện pháp phòng ngừa)
Flood damage (tương tự như SYN Flood – làm tràn ngập các request tới hệ thống)	H (Gây gián đoạn dịch vụ đang cung cấp)	L (Do các doanh nghiệp khi thiết kế hệ thống thường sẽ có các biện pháp ngăn chặn)	Thiết lập mức tối đa	L
Trộm cắp tài sản thông tin (vật lý)	H	L (Do các doanh nghiệp thường sẽ có các quy định về bảo mật cũng như phương thức tiếp cận thông tin)	Chìa khóa, bảo vệ	L
Xâm nhập logic	H	M	Các hệ thống phát hiện và ngăn chặn xâm nhập	L

VI

GHI LẠI KẾT QUẢ ĐÁNH GIÁ RỦI RO

V. VIẾT BÁO CÁO KẾT QUẢ ĐÁNH GIÁ RỦI RO

Mục tiêu của đánh giá rủi ro là phát hiện các tài sản và các rủi ro liên quan để tạo bảng xếp hạng chúng.

Tài sản	Ảnh hưởng đến tài sản	Lỗ hổng	Khả năng xảy ra lỗ hổng	Nhân tố Đánh giá rủi ro
Khách hàng yêu cầu dịch vu qua e-mail (Đến)	55	E-mail bị gián đoạn do lỗi phần cứng	0.2	11
Khách hàng yêu cầu dịch vu qua e-mail (Đến)	55	E-mail bị gián đoạn do lỗi phần mềm	0.2	11
Khách hàng yêu cầu dịch vu qua SSL (Đến)	100	Mất yêu cầu khách hàng do lỗi phần cứng Web Server	0.1	10
Khách hàng yêu cầu dịch vu qua SSL (Đến)	100	Mất yêu cầu khách hàng do lỗi dịch vụ Web Server hoặc ISP	0.1	10
Khách hàng yêu cầu dịch vu qua e-mail (Đến)	55	E-mail bị gián đoạn do tấn công SMTP vào Server	0.1	5.5

Bảng xếp hạng rủi ro lỗ hổng bảo mật

V. VIẾT BÁO CÁO KẾT QUẢ ĐÁNH GIÁ RỦI RO

Tài sản	Ảnh hưởng đến tài sản	Lỗ hổng	Khả năng xảy ra lỗ hổng	Nhân tố Đánh giá rủi ro
Khách hàng yêu cầu dịch vu qua e-mail (Đến)	55	E-mail bị gián đoạn do lỗi phần cứng	0.2	11
Khách hàng yêu cầu dịch vu qua e-mail (Đến)	55	E-mail bị gián đoạn do lỗi phần mềm	0.2	11
Khách hàng yêu cầu dịch vu qua SSL (Đến)	100	Mất yêu cầu khách hàng do lỗi phần cứng Web Server	0.1	10
Khách hàng yêu cầu dịch vu qua SSL (Đến)	100	Mất yêu cầu khách hàng do lỗi dịch vụ Web Server hoặc ISP	0.1	10
Khách hàng yêu cầu dịch vu qua e-mail (Đến)	55	E-mail bị gián đoạn do tấn công SMTP vào Server	0.1	5.5
Khách hàng yêu cầu dịch vu qua e-mail (Đến)	55	E-mail bị gián đoạn do lỗi dịch vụ ISP	0.1	5.5
Khách hàng yêu cầu dịch vu qua e-mail (Đến)	55	E-mail bị gián đoạn do mất điện	0.1	5.5
Khách hàng yêu cầu dịch vu qua SSL (Đến)	100	Mất yêu cầu khách hàng do bị tấn công DOS	0.025	2.5
Khách hàng yêu cầu dịch vu qua SSL (Đến)	100	Mất yêu cầu khách hàng do lỗi phần mềm Web Server	0.1	1
Khách hàng yêu cầu dịch vu qua SSL (Đến)	100	Mất yêu cầu khách hàng do bị tấn công Tràn bộ đệm	0.1	1

Bảng xếp hạng rủi ro lỗ hổng bảo mật

Sản phẩm	Mục đích
Bảng phân loại tài sản thông tin	Thu thập thông tin về tài sản thông tin và tác động hoặc giá trị của chúng đối với tổ chức
Bảng phân tích tiêu chí có trọng số	Chỉ định giá trị được xếp hạng hoặc trọng số tác động cho mỗi tài sản thông tin
Bảng tính TVA	Kết hợp đầu ra từ việc xác định và ưu tiên tài sản thông tin với việc xác định và ưu tiên các mối đe dọa và xác định các lỗ hổng tiềm ẩn trong “bộ ba”; cũng như kết hợp chặt chẽ các biện pháp kiểm soát hiện có và đã được lên kế hoạch
Bảng xếp hạng rủi ro lỗ hổng bảo mật	Chỉ định giá trị xếp hạng theo mức độ rủi ro cho từng cặp tài sản - lỗ hổng không được kiểm soát

Bảng 8.14. Sản phẩm của việc xác định và đánh giá rủi ro.

VI. TÓM TẮT CHƯƠNG

- Quản lý rủi ro, kiểm tra, lập hồ sơ về tài sản thông tin.
- Ban Quản Lý xác định và kiểm soát rủi ro. Nhóm InfoSec quản lý rủi ro.
- Cần xác định, phân loại và ưu tiên các tài sản thông tin qua việc đánh giá, gán trọng số cho chúng.
- Kiểm tra, đánh giá các mối đe dọa mỗi tài sản phải đối mặt
  - ➔ Danh sách tài sản thông tin và lỗ hổng bảo mật
- Bảng Threats-Vulnerabilities-Assets (TVA) để kiểm tra "mức độ tiếp xúc" của tài sản, đánh giá mức độ dễ bị tổn thương một cách đơn giản.

VI. TÓM TẮT CHƯƠNG

- Đánh giá rủi ro nhằm ấn định xếp hạng rủi ro hoặc điểm số hóa rủi ro với một lỗ hổng cụ thể của một tài sản.
- Các biện pháp kiểm soát, bảo vệ và đối phó cần được xác định cho từng mối đe dọa và lỗ hổng liên quan.
- Ba loại kiểm soát: chính sách, chương trình và công nghệ.
- Kiểm soát truy cập gồm: bắt buộc, tùy ý hoặc không tùy ý.
- Quá trình xác định rủi ro cần chỉ định báo cáo phục vụ cho chức năng gì, ai chuẩn bị, ai đánh giá
- Bảng TVA và bảng xếp hạng rủi ro dễ bị tổn thương là tài liệu làm việc ban đầu cho bước tiếp theo trong quy trình quản lý rủi ro: đánh giá và kiểm soát rủi ro.