Chapter 1: Security & Risk Management

Technology Brief

Bảo mật & Quản lý rủi ro là lĩnh vực đầu tiên của chứng chỉ CISSP. Quản lý an ninh và rủi ro liên quan đến các tài nguyên có giá trị như tài sản thông tin. Thông tin hoặc dữ liệu luôn là tài sản quan trọng của một tổ chức. Bất kỳ sự xâm phạm nào đối với thông tin nhạy cảm hoặc bất kỳ tài sản nào khác dẫn đến mất dữ liệu của một tổ chức dẫn đến tổn thất tài chính và nó cũng ảnh hưởng đến sự ổn định của tổ chức. Tài sản có thể là bất kỳ tài nguyên có giá trị nào của một tổ chức, nhưng chúng ta sẽ thảo luận về các tài sản liên quan đến hệ thống thông tin.

Chương này bao gồm các khái niệm và ứng dụng của tính bảo mật, tính toàn vẹn và tính sẵn có với việc đánh giá việc áp dụng các nguyên tắc, chính sách và tiêu chuẩn quản trị an ninh. Các vấn đề pháp lý và quy định, đạo đức nghề nghiệp, các yêu cầu của cộng đồng doanh nghiệp, các khái niệm & phương pháp quản lý rủi ro với mô hình hóa mối đe dọa (threat modeing) được đề cập trong chương này.

Security Concepts

Valuable Information Assets

Bảo mật những tài sản là một khía cạnh quan trọng của môi trường an toàn thông tin. Tuy nhiên, bảo đảm liên quan trực tiếp đến giá trị của tài sản. Các tài sản có giá trị lớn hơn yêu cầu bảo mật nhiều hơn và do đó, chi phí nhiều hơn. *Nếu một tổ chức không có bất kỳ thông tin có giá trị nào hoặc thông tin không nhạy cảm thì họ không được phép chi nhiều tiền cho việc bảo mật so với các doanh nghiệp khác có thông tin rất nhạy cảm và tài sản có giá trị cao*.

An asset là bất cứ thứ gì có giá trị đối với một tổ chức. Nó có thể thay đổi từ các mục hữu hình (con người, máy tính và nhiều hơn nữa) đến các mục vô hình (như thông tin cơ sở dữ liệu). Biết được giá trị và bản chất chính xác của tài sản giúp xác định phạm vi bảo mật mà chúng ta cần thực hiện.

Tangible Assets

Tài sản hữu hình là những nguồn thông tin quý giá, có giá trị vật chất và giá trị cao đối với doanh nghiệp. Các tài sản vật lý này có thể bao gồm *ổ cứng, máy chủ, trung tâm dữ liệu, tài liệu in, tệp và các tài nguyên lưu trữ dữ liệu khác*. Những tài sản này có thể bị đánh cắp, phá hủy hoặc xâm nhập gây ra tổn thất tiền bạc cho tổ chức.

Intangible Assets

Tài sản vô hình là tài sản phi vật chất. Danh mục này bao gồm các tài sản như *phần mềm, mã nguồn, tài sản trí tuệ của một tổ chức & đó là bí mật thương mại*. Danh mục này cũng bao gồm thông tin nhận dạng cá nhân như thông tin cá nhân của khách hàng.

CIA Triad

Confidentiality

Chúng ta muốn đảm bảo rằng dữ liệu bí mật và nhạy cảm của Chúng ta được bảo mật. Bí mật có nghĩa là mà chỉ những người được ủy quyền mới có thể làm việc và xem các tài nguyên kỹ thuật số của cơ sở hạ tầng của chúng tôi. *Điều này cũng ngụ ý rằng những người không được phép không được có bất kỳ quyền truy cập nào vào dữ liệu*. Nói chung, có hai loại dữ liệu: dữ liệu chuyển động khi nó di chuyển trên mạng và dữ liệu ở trạng thái nghỉ, khi dữ liệu nằm trong bất kỳ bộ lưu trữ phương tiện nào (chẳng hạn như máy chủ, ổ cứng cục bộ, đám mây). Đối với dữ liệu đang chuyển động, chúng ta cần đảm bảo mã hóa dữ liệu trước khi gửi qua mạng. Một tùy chọn khác mà Chúng ta có thể sử dụng cùng với mã hóa là sử dụng một mạng riêng cho dữ liệu nhạy cảm. Đối với dữ liệu ở trạng thái nghỉ, Chúng ta có thể áp dụng mã hóa tại ổ đĩa phương tiện lưu trữ để không ai có thể đọc được trong trường hợp bị đánh cắp.

Implementation of Confidentiality

Bảo mật có thể được thực hiện bằng cách sử dụng kiểm soát truy cập và mật mã. Kiểm soát truy cập có thể ở dạng kiểm soát truy cập được định cấu hình trên thiết bị bảo mật hoặc kiểm soát và giám sát vật lý việc truy cập của người dùng trái phép và những kẻ tấn công đối với các tài sản hữu hình. Mật mã giúp bảo vệ khỏi việc tiết lộ thông tin cho người dùng trái phép. Dạng dữ liệu được mã hóa chỉ có thể được giải mã bởi người dùng hợp pháp mà dữ liệu được sử dụng.

Integrity

Chúng ta không muốn những người không có thẩm quyền có thể truy cập hoặc thao túng dữ liệu của mình. Tính toàn vẹn của dữ liệu đảm bảo rằng dữ liệu ở dạng ban đầu và chỉ các bên được ủy quyền mới có thể sửa đổi dữ liệu. Tính toàn vẹn liên quan đến tính xác thực và độ chính xác của thông tin. Tính toàn vẹn của thông tin đảm bảo rằng thông tin đến từ một nguồn xác thực, đáng tin cậy và để xác minh tính chính xác của dữ liệu.

Implementation of Integrity

Tính toàn vẹn có thể được thực hiện một cách bí mật để ngăn chặn bất kỳ truy cập trái phép nào dẫn đến việc truy cập và sửa đổi dữ liệu. Sử dụng kiểm soát truy cập & mật mã, chúng ta có thể đạt được sự bảo vệ toàn vẹn cơ bản; tuy nhiên, để triển khai tính toàn vẹn một cách an toàn, cần có các tiêu chuẩn Hashing / Message. Các thuật toán toán học này tính toán một giá trị thông báo, được so sánh để xác minh tính toàn vẹn. Nếu một bit trong dữ liệu được sửa đổi, giá trị được tính toán của thông báo thông báo sẽ khác với giá trị thông báo đã nhận.

Chúng ta có thể sử dụng thuật ngữ **"CIA"** để ghi nhớ những khái niệm bảo mật cơ bản nhưng quan trọng nhất này.

CIA	Risk	Control
Confidentiality	The risk of privacy loss. Unauthorized disclosure.	Encryption. Authentication. Access Control
Integrity	Modified data by an unauthorized source	Access Control, Cryptography along with Hashing & Message Digests
Availability	Unavailability of resources & information for authorized users	Backups, High-Availability, Fault Tolerance, Co-location

Table 1-01: Risk and Its Protection by Implementing CIA

Availability

Tính khả dụng là khả năng tiếp cận thông tin. Bất cứ khi nào người dùng được ủy quyền yêu cầu thông tin này, thông tin đó phải có sẵn cho anh ta. Tính khả dụng áp dụng cho các hệ thống và dữ liệu. Nếu những người được ủy quyền không thể lấy được dữ liệu do lỗi mạng chung hoặc do tấn công từ chối dịch vụ (DOS), thì đó là một vấn đề miễn là doanh nghiệp có liên quan. Nó cũng có thể dẫn đến mất doanh thu hoặc ghi nhận một số kết quả quan trọng.

Implementation of High-Availability

Các đường dẫn dự phòng được định cấu hình để thiết kế một mạng có tính khả dụng cao. Lưu trữ thông tin ở nhiều vị trí cũng sẽ giúp mang lại tính khả dụng cao. Một phương pháp khác để đạt được tính khả dụng là khả năng chịu lỗi. Định cấu hình các liên kết dự phòng để khắc phục sự cố của các liên kết giúp tránh tình trạng không có tài nguyên.

Security Governance Principles

Quản trị an ninh là một nguyên tắc quan trọng mà mọi tổ chức nên tuân theo. Một tổ chức có quản trị an ninh tập trung vào bảo mật tài sản của họ bằng cách thiết lập một khuôn khổ, đảm bảo các quyết định phù hợp để bảo đảm tài sản. Khuôn khổ quản trị bảo mật & trách nhiệm giải trình điều chỉnh quy trình của một tổ chức với các chiến lược, triển khai các tiêu chuẩn và chính sách cũng như quản lý các trách nhiệm. Các tổ chức quản trị của bên thứ ba như Viện Tiêu chuẩn & Công nghệ Quốc gia cung cấp các khuôn khổ được các tổ chức sử dụng để thực hành tốt nhất.

“The key goal of information security is to reduce adverse impacts on the organization to an acceptable level.”

Sau đây là một số phương pháp và khuôn khổ quản lý bảo mật khác dành cho các chuyên gia bảo mật, bao gồm các tiêu chuẩn phát triển, kiến trúc bảo mật, kiểm soát bảo mật, phương pháp quản trị và quy trình quản lý:

- ISO / IEC 17799: 2005 Công nghệ thông tin - Kỹ thuật bảo mật - Quy tắc thực hành về quản lý an toàn thông tin
- Dòng hệ thống quản lý an toàn thông tin theo tiêu chuẩn ISO / IEC 27000
- Quản lý bảo mật thông tin ISO / IEC 27001
- ISO / IEC 27002 Công nghệ thông tin - Kỹ thuật bảo mật - Quy tắc thực hành về kiểm soát an toàn thông tin
- Tiêu chí chung (CC) hoặc ISO / IEC 15408
- Thư viện Cơ sở hạ tầng Công nghệ Thông tin (ITIL)
- Khung Zachman
- TOGAF
- DoDAF
- MODAF
- COBIT

Khung quản trị bao gồm việc phân công vai trò, trách nhiệm, quyền hạn, ngân sách và nguồn lực. Khi mới thành lập, tổ chức không có đủ thông tin có giá trị nhưng khi tổ chức phát triển, thông tin có giá trị tăng lên đòi hỏi một khuôn khổ quản trị phù hợp. Khung Quản trị Bảo mật đã thiết lập một khuôn khổ bảo mật bao gồm các chính sách và quy trình bảo mật được xác định rõ ràng, đánh giá rủi ro, quản lý rủi ro, các chính sách và hợp đồng được lập thành văn bản giữa

nhân viên, nhân viên và các bên thứ ba. Việc giám sát tất cả các hoạt động này, vi phạm và thực hiện các hành động khắc phục cũng bao gồm trong khuôn khổ quản trị. Sau đây là phạm vi và mục tiêu cơ bản của khung quản trị bảo mật CNTT:

- Rủi ro và mối đe dọa đối với doanh nghiệp luôn là mối nguy hiểm và có thể có tác động đáng kể đến danh tiếng và sự ổn định.
- Tác động về uy tín & tài chính có thể đáng kể.
- Thực thi bảo mật thông tin hiệu quả đòi hỏi các hành động phối hợp và tích hợp từ trên xuống.
- Các quy tắc, chính sách và ưu tiên cần được xác định và thực thi một cách hiệu quả.

Organizational Processes

Để hiểu các quy trình của một tổ chức, hãy xem xét quy trình sau:

Acquisition

Quá trình mua lại là khi hai tổ chức quyết định hợp nhất thành một tổ chức hoặc khi một tổ chức mua một tổ chức khác. Kịch bản này đưa các chuyên gia bảo mật xem xét các quy trình quản lý để đảm bảo rằng an ninh của tổ chức không bị ảnh hưởng từ việc sáp nhập này. Việc sáp nhập có thể mang lại công nghệ hiện đại, tạo ra các vấn đề tương thích hoặc công nghệ cũ hơn tạo ra các vấn đề bảo mật. Tương tự, việc hợp nhất hai tổ chức có thể yêu cầu nâng cấp bảo mật nếu tổ chức hợp nhất có nhiều tài sản có giá trị hơn.

Một cân nhắc quan trọng khác đối với các chuyên gia bảo mật là nhận thức về các quy tắc, quy định, chính sách và đào tạo nâng cao nhận thức về bảo mật. Có thể có khả năng nhân viên của tổ chức hợp nhất không hiểu rõ về cơ sở hạ tầng và chính sách bảo mật.

Cân nhắc cuối cùng trong việc mua lại là phát triển và triển khai các quy tắc, quy định và chính sách mới cho các tổ chức mới. Việc gia hạn hợp đồng với bên thứ ba và các mối quan hệ cần được xem xét lại.

Divestiture

Việc thoái vốn là một quá trình khi một bộ phận của tổ chức được bán hoặc tách ra. Đó là một thách thức đối với một chuyên gia bảo mật để đảm bảo an ninh. Khi việc chuyển nhượng ảnh hưởng đến nhân sự, khả năng rò rỉ dữ liệu sẽ tăng lên. Để giảm thiểu, chỉ những nhân viên hiện tại mới có quyền truy cập vào các tài nguyên. Quyền truy cập và đặc quyền của những nhân viên đã tham gia vào công việc này nên bị loại bỏ hoặc hạn chế.

Governance Committees

Các Ủy ban quản trị của một tổ chức có quyền quản lý việc quản trị.

Ủy ban có thể tuyển dụng, ủy quyền và đưa ra quyết định. Chuyên gia bảo mật phải giải thích cho họ những rủi ro đối với một tổ chức và các biện pháp an ninh của họ.

Organizational Roles and Responsibilities

Trong một tổ chức, lĩnh vực quan trọng và tập trung nhất của quản lý là phân chia vai trò và trách nhiệm. Trước khi phân chia trách nhiệm cho các cá nhân, cần hiểu rõ cơ cấu tổ chức và hệ thống cấp bậc. Hệ thống phân cấp và cấu trúc là những nguyên tắc cơ bản để phát triển bất kỳ tổ chức nào. Cấu trúc của một tổ chức là một chuỗi phân cấp, phân chia các vai trò, trách nhiệm, cấp độ và quyền hạn khác nhau giữa các cá nhân liên quan đến tổ chức.

Việc phân chia hiệu quả các vai trò và trách nhiệm của tổ chức sẽ có lợi về mặt:

- Tạo điều kiện thuận lợi để đạt được các mục tiêu
- Điều phối tất cả các hoạt động
- Giảm xung đột tổng thể
- Loại bỏ sự chồng chéo của các quy trình
- Giao tiếp tốt hơn ở mọi cấp độ của cơ cấu tổ chức
- Lập kế hoạch hiệu quả
- Khuyến khích sự sáng tạo

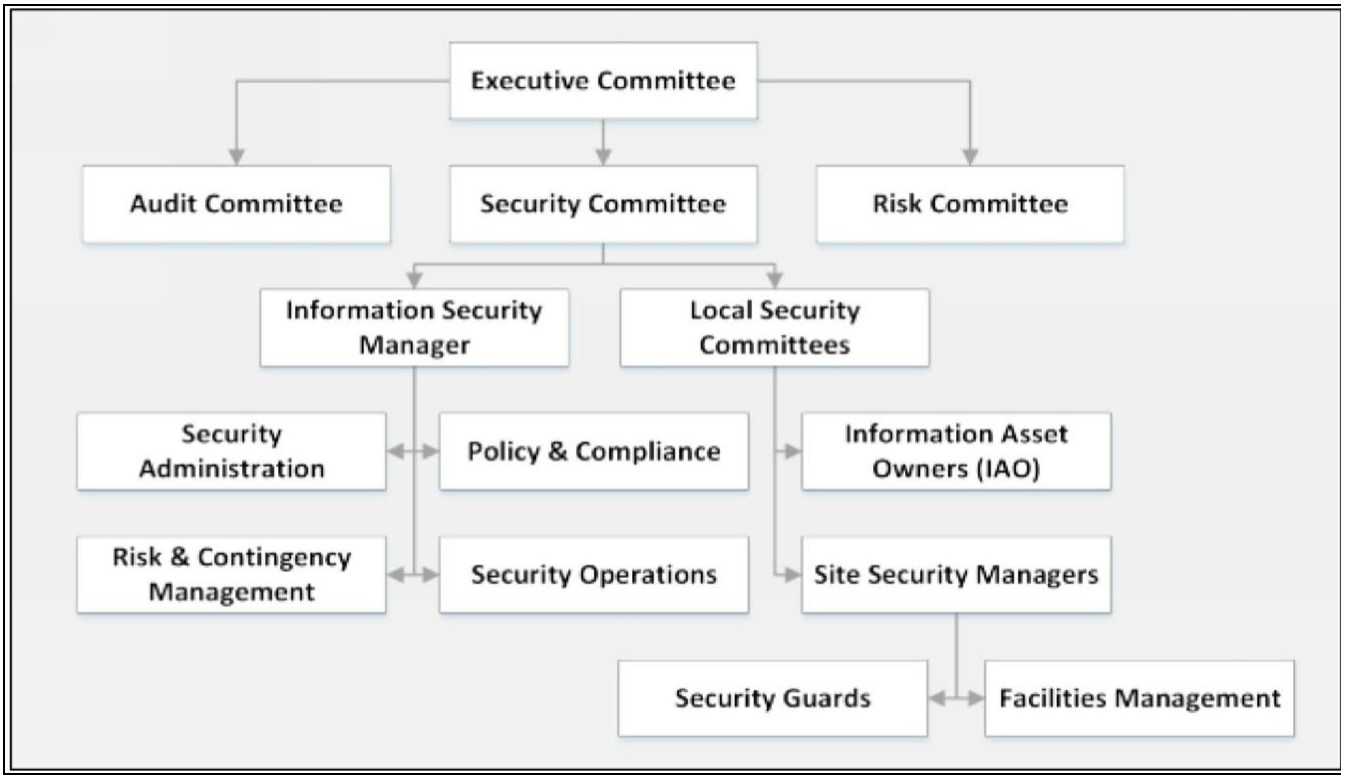


Figure 3. ISO27000-General Organizational Structure

Board of Directors

Hội đồng quản trị là một ủy ban gồm các giám đốc, chịu trách nhiệm cuối cùng trong việc điều hành công ty. Các bộ phận quản lý và bộ phận bảo mật thông tin là những lĩnh vực không thể thiếu của quản trị này. Các trách nhiệm độc quyền được giao cho các giám đốc điều hành do Giám đốc điều hành (CEO) lãnh đạo.

Executive Directors

Giám đốc điều hành chịu trách nhiệm phê duyệt các kế hoạch chiến lược tổng thể và bắt buộc các nguyên tắc bảo mật. Giám đốc điều hành đang làm việc với Ủy ban bảo mật (SC), Giám đốc an ninh, ISM, Kiểm toán viên và những người khác để đảm bảo rằng các chính sách phù hợp được thực thi.

Chief Security Officer (CSO)

Sau đây là những trách nhiệm chính và phổ biến nhất của Giám đốc An ninh (SCO).

- CSO chịu trách nhiệm giám sát, động viên và chỉ đạo các ủy ban an ninh.
- Đi đầu trong quản trị thông tin.
- Cung cấp các định hướng chiến lược tổng thể, hỗ trợ và giám sát các quy trình.
- Theo dõi & quản lý Quản lý bảo mật thông tin (ISM).

Information Security Management (ISM)

Cơ quan quản lý bảo mật thông tin (ISM) chịu trách nhiệm về:

- Duy trì các tiêu chuẩn, quy trình và hướng dẫn về an toàn thông tin kỹ thuật và phi kỹ thuật.
- Rà soát và giám sát việc tuân thủ các tuyên bố chính sách.
- Đóng góp vào quy trình Tự đánh giá và Kiểm soát Nội bộ (CSA).
- Hỗ trợ các IAO và các nhà quản lý trong việc thực hiện các kiểm soát, quy trình và công cụ hỗ trợ.
- Chịu trách nhiệm hỗ trợ IAO trong việc điều tra và khắc phục các sự cố an toàn thông tin hoặc các vi phạm chính sách khác.
- Thu thập và phân tích các chỉ số và sự cố an toàn thông tin.
- Chịu trách nhiệm về các trách nhiệm khác liên quan đến bảo mật thông tin.

Managers

Người quản lý chịu trách nhiệm về:

- Thực thi các chính sách bảo mật thông tin theo sổ tay bảo mật đã được phê duyệt.
- Đảm bảo hiệu quả và sức mạnh của các biện pháp kiểm soát an ninh vật lý và kỹ thuật được triển khai.
- Đảm bảo rằng nhân viên đang tuân thủ tất cả các chính sách.
- Thông báo cho nhân viên về các chính sách của công ty, cung cấp nhận thức và đào tạo.
- Cập nhật hoặc báo cáo Quản lý bảo mật thông tin.
- Thông báo kịp thời cho ISM về bất kỳ vi phạm chính sách nào.
- Chịu trách nhiệm đánh giá sự tuân thủ.
- Thực hiện Quy trình CSA & Kiểm toán Nội bộ.

Information Asset Owners (IAOs)

Chủ sở hữu tài sản thông tin (IAO) là những cá nhân, thường là người quản lý, chịu trách nhiệm bảo vệ tài sản thông tin. Họ chịu trách nhiệm về bảo mật này bởi Ủy ban Bảo mật (SC) hoặc Ủy ban An ninh địa phương (LSC). Các trách nhiệm chính của IOA là:

- Phân loại và Bảo vệ tài sản thông tin
- Quản lý Kiểm soát Chủ động
- Cấp phép truy cập vào tài sản thông tin theo yêu cầu
- Giám sát việc tuân thủ và các yêu cầu bảo vệ, ảnh hưởng đến tài sản

End-Users

Trách nhiệm của Người dùng cuối như sau:

- Họ có trách nhiệm tuân thủ tất cả các yêu cầu và chính sách bảo mật của một tổ chức.
- Chịu trách nhiệm tuân thủ các yêu cầu theo hợp đồng (chẳng hạn như thỏa thuận không tiết lộ và Thỏa thuận mức dịch vụ).
- Trách nhiệm đạo đức về an toàn thông tin nhạy cảm của tổ chức và tài sản thông tin.

- Tham gia các khóa đào tạo và nâng cao nhận thức về an toàn thông tin.
- Báo cáo bất kỳ hoạt động đáng ngờ nào, vi phạm bảo mật, sự cố bảo mật hoặc

lo ngại về an ninh cho nhân viên thích hợp.

Compliance Requirement

Trong hai thập kỷ trước, vi phạm an toàn thông tin cần bảo mật mới liên quan đến khuôn khổ pháp lý và quy định hoặc cập nhật cho khuôn khổ pháp lý và quy định hiện có để bao gồm các yêu cầu tuân thủ liên quan đến bảo mật ở các quốc gia khác nhau. Các yêu cầu tuân thủ các khuôn khổ pháp lý và lập pháp đã tăng lên một cách linh hoạt do tính chất toàn cầu của các dịch vụ internet, trao đổi thông tin qua biên giới và các dịch vụ thương mại điện tử. Sau đây là một số điều khoản pháp lý và lập pháp quan trọng đối với lĩnh vực Bảo mật thông tin.

Legislative and Regulatory Compliance

Hệ thống pháp luật sử dụng thông luật được gọi là hệ thống pháp luật thông luật; thông luật dựa trên các quyết định của tòa án. Các quốc gia như Vương quốc Anh, Hoa Kỳ, Canada, Úc, Nam Phi, Ấn Độ, Malaysia, Singapore và Hồng Kông tuân theo luật chung.

Nói chung, ba loại được thiết lập theo luật chung:

1. **Regulatory law:** Nó còn được gọi là luật Hành chính. Nó giải quyết các quy định của các cơ quan hành chính của chính phủ. Luật lập pháp, quy chế lập pháp là một hệ thống pháp luật được giải quyết bởi nhánh lập pháp của chính phủ.

2. **Criminal law:** đối phó với các vi phạm pháp luật của chính phủ. Luật tôn giáo là hệ thống pháp luật dựa trên các nguyên tắc tôn giáo. Ví dụ: đạo luật Hồi giáo, đạo Hindu và đạo Thiên chúa.

3. **Civil law:** giải quyết các vụ kiện của các bên tư nhân. Luật dân sự là một hệ thống pháp luật dựa trên luật được pháp điển hóa và đối lập với thông luật. Các quốc gia như Pháp, Đức và các quốc gia khác tuân theo luật dân sự.

Privacy Requirements in Compliance

Quyền riêng tư là bảo vệ Thông tin nhận dạng cá nhân (PII) hoặc Thông tin cá nhân nhạy cảm (SPI) có thể được sử dụng để xác định một người trong ngữ cảnh với một nhóm hoặc cá nhân.

National Institute of Standards and Technology (NIST)

NIST đang xuất bản một hướng dẫn để bảo vệ tính bí mật của Thông tin Nhận dạng Cá nhân. Theo ấn phẩm đặc biệt 800-122 của NIST, Personally

Thông tin nhận dạng (PII) được định nghĩa là:

1. Bất kỳ thông tin nào có thể được sử dụng để tìm ra danh tính của cá nhân, chẳng hạn như tên, số an sinh xã hội, ngày tháng và nơi sinh của người đó hoặc hồ sơ sinh trắc học.
2. Bất kỳ thông tin nào thuộc về một cá nhân như thông tin y tế, giáo dục, tài chính và việc làm.

Privacy Laws

Luật bảo mật đề cập đến việc bảo vệ và duy trì các quyền riêng tư của cá nhân. Luật về quyền riêng tư ở Hoa Kỳ bao gồm những điều sau đây:

- Đạo luật về trách nhiệm giải trình và cung cấp bảo hiểm y tế (HIPAA)
- Đạo luật hiện đại hóa dịch vụ tài chính (GLB), 15 Mã Hoa Kỳ: 6801-6810
- Quy tắc cuối cùng về quyền riêng tư của thông tin tài chính của người tiêu dùng, 16 Bộ luật về quy định liên bang, Phần 313

Ở Vương quốc Anh, chúng bao gồm những điều sau đây:

- Đạo luật bảo vệ dữ liệu 1998 (Vương quốc Anh)
- Chỉ thị bảo vệ dữ liệu (Liên minh Châu Âu)

Legal & Regulatory Issues

Sự xâm phạm thông tin có thể dẫn đến trách nhiệm dân sự hoặc hình sự đối với một phần của tổ chức sẽ được nhóm lại theo các vấn đề pháp lý và quy định.

Danh sách các vấn đề sau đây có thể có ý nghĩa pháp lý hoặc quy định.

Cyber Crime

Các hoạt động phạm tội được thực hiện qua các mạng truyền thông, chẳng hạn như Internet, điện thoại, mạng không dây, vệ tinh và mạng di động được gọi là tội phạm mạng.

Cyber Terrorism

Khủng bố mạng là một loại tội phạm mạng nhằm vào máy tính và mạng máy tính và thường được tính toán trước về bản chất. Mục tiêu chính của các cuộc tấn công này có thể là gây hại dựa trên các hình thức xã hội, hệ tư tưởng, tôn giáo, chính trị hoặc tương tự.

Cyber Stalking

Cyber Stalking là một loại tội phạm mạng, trong đó tội phạm quấy rối hoặc đe dọa nạn nhân bằng cách sử dụng Internet và các tài nguyên điện tử khác.

Information Warfare

Chiến tranh thông tin là một loại tội phạm mạng nhằm gây mất ổn định đối phương, chẳng hạn như các tập đoàn và tổ chức để đạt được lợi thế cạnh tranh. Ví dụ: tuyên truyền sai trái, làm xấu mặt trang web, v.v..

Denial-Of-Service (DoS) attack or Distributed Denial-Of-Service (DDoS)

Các cuộc tấn công DoS / DDoS là tội phạm mạng trong đó các trang web của hệ thống máy tính của bất kỳ người dùng nào không thể truy cập được bằng cách sử dụng nhiều dịch vụ yêu cầu làm quá tải máy chủ web và ứng dụng.

Các ví dụ sau đây sẽ làm cho tội phạm mạng dễ hiểu hơn.

Phishing là một loại tội phạm mạng trong đó người dùng bị dụ đến một kẻ tấn công đã xây dựng trang web bất hợp pháp trông giống với trang web thực tế mà người dùng định truy cập. Ví dụ, các trang web ngân hàng trực tuyến, trang đăng nhập e-mail, v.v. Một cuộc tấn công lừa đảo thành công sẽ dẫn đến việc kẻ tấn công chiếm được thông tin đăng nhập của người dùng.

Pharming là một kiểu tấn công mạng trong đó người dùng được chuyển hướng đến một trang web độc hại do kẻ tấn công tạo ra. Nói chung, loại chuyển hướng này xảy ra mà người dùng không chấp nhận hoặc không biết.

SMiShing / SMS Phishing là một kiểu tấn công mạng sử dụng mạng di động. Trong cuộc tấn công này, Dịch vụ nhắn tin ngắn (SMS) được sử dụng để thu hút người dùng đến các trang web độc hại do kẻ tấn công tạo ra. Điều này tương tự như lừa đảo.

Data Breaches

Vi phạm dữ liệu là một sự kiện bảo mật trong đó dữ liệu nhạy cảm, được bảo vệ hoặc bí mật

sao chép, truyền, xem, đánh cắp hoặc sử dụng trái phép bởi một cá nhân không được phép cho các mục đích khác nhau. Nó cũng có thể là do vô tình tiết lộ thông tin, rò rỉ dữ liệu hoặc tràn dữ liệu. Việc vi phạm dữ liệu có thể xảy ra do thực hiện các hành vi phi đạo đức như hack, tội phạm có tổ chức, sơ suất trong việc xử lý phương tiện, v.v.

Vi phạm dữ liệu là một sự cố bảo mật. Do đó, nhiều khu vực pháp lý đã thông qua luật thông báo vi phạm dữ liệu. Tại Hoa Kỳ, luật liên quan đến vi phạm dữ liệu được phân loại là luật vi phạm bảo mật.

Transborder Data Flow

Việc chuyển dữ liệu được máy tính hóa qua biên giới quốc gia, tiểu bang hoặc ranh giới chính trị được gọi là luồng dữ liệu xuyên thứ tự. Dữ liệu có thể là cá nhân, doanh nghiệp, kỹ thuật và tổ chức. Các vấn đề pháp lý có thể phát sinh liên quan đến quyền sở hữu và sử dụng dữ liệu đó.

Licensing and Intellectual Property

Sở hữu trí tuệ (IP) đề cập đến các tác phẩm sáng tạo như thiết kế, âm nhạc, tác phẩm văn học, nghệ thuật, phát minh, v.v. Người tạo ra các tác phẩm trí tuệ này có độc quyền nhất định đối với tài sản. Các quyền độc quyền này được gọi là Quyền sở hữu trí tuệ (IPR). Luật sở hữu trí tuệ là luật pháp lý chịu trách nhiệm về Quyền sở hữu trí tuệ (IPR).

Dưới đây là một số thuật ngữ liên quan đến IPR:

Copyright

Sở hữu trí tuệ trao quyền đặc biệt cho người tạo ra tác phẩm gốc và những người khác không có quyền sao chép tác phẩm đó. Bản quyền dành riêng cho từng quốc gia.

Patent

Một tập hợp các quyền đặc biệt được cấp cho người phát minh ra các phát minh mới, hữu ích, sáng tạo và có thể áp dụng trong ngành. Quyền này ngăn cản người khác chế tạo, sử dụng, bán hoặc nhập khẩu sáng chế. Bằng sáng chế là một tài liệu công khai và được cấp trong một thời hạn cụ thể.

Trademark

Một biểu tượng hoặc nhãn hiệu duy nhất được sử dụng để đại diện cho sản phẩm của một cá nhân hoặc tổ chức.

Trade Secret

Công thức, thiết kế hoặc quy trình phải được bảo vệ để tránh thông tin bị sao chép.

Importing and Exporting Controls

Nhiều quốc gia có những hạn chế về xuất nhập khẩu liên quan đến việc mã hóa dữ liệu. Ví dụ: các mục mã hóa được thiết kế, phát triển, cấu hình, điều chỉnh hoặc sửa đổi đặc biệt cho các ứng dụng quân sự, chỉ huy, điều khiển và ứng dụng tình báo thường được kiểm soát dựa trên danh sách bom, đạn.

Professional Ethics

Nghề bảo mật thông tin dựa trên sự tin tưởng, vì các chuyên gia có thể đang xử lý thông tin nhạy cảm hoặc bí mật. Các quy tắc đạo đức nghề nghiệp lành mạnh và được áp dụng nhất quán cần được các chuyên gia tuân thủ.

(ISC)² code of Professional Ethics

Tổ chức Chứng nhận Bảo mật Hệ thống Thông tin Quốc tế (ISC)² có một bộ quy tắc đạo đức nghề nghiệp được công bố cho các thành viên của mình. (ISC)² Quy tắc đạo đức bao gồm một phần mở đầu bắt buộc và bốn quy tắc bắt buộc.

Các quy tắc được liệt kê theo thứ tự ưu tiên; do đó, bất kỳ xung đột nào nên được giải quyết theo trình tự được trình bày dưới đây:

1. Bảo vệ xã hội, thịnh vượng chung và cơ sở hạ tầng
2. Hành động một cách danh dự, trung thực, chính đáng, có trách nhiệm và hợp pháp
3. Cung cấp dịch vụ chuyên cần và có năng lực cho hiệu trưởng
4. Thăng tiến và bảo vệ nghề nghiệp

Protect society, the commonwealth, and the infrastructure

Trọng tâm của quy tắc đầu tiên là công chúng, sự hiểu biết của họ và sự tin tưởng vào một hệ thống thông tin. Các chuyên gia bảo mật chịu trách nhiệm thúc đẩy các phương pháp bảo mật an toàn và cải thiện cơ sở hạ tầng và bảo mật hệ thống cho sự tin tưởng của công chúng.

Act honorably, honestly, justly, responsibly, and legally

Quy tắc này rất đơn giản, nhưng có một số điểm của quy tắc này đáng được thông báo ở đây, một điểm được nêu chi tiết trong quy tắc này và có liên quan đến các luật từ các khu vực pháp lý khác nhau bị phát hiện là xung đột. (ISC) 2® Code of Ethics gợi ý rằng quyền ưu tiên được dành cho khu vực tài phán mà các dịch vụ đang được cung cấp. Một điểm khác của quy chuẩn này liên quan đến việc cung cấp lời khuyên sáng suốt và cảnh báo các chuyên gia bảo mật khỏi việc thúc đẩy sự sợ hãi, không chắc chắn và nghi ngờ một cách không cần thiết..

Provide diligent and competent service to principals

Trọng tâm của quy chuẩn này là đảm bảo rằng các chuyên gia bảo mật cung cấp các dịch vụ có thẩm quyền đủ điều kiện và duy trì giá trị và tính bảo mật của thông tin và các hệ thống liên quan. Một cân nhắc quan trọng bổ sung là đảm bảo rằng các chuyên gia không có xung đột lợi ích trong việc cung cấp các dịch vụ chất lượng.

Advance and protect the profession

Quy định này yêu cầu các chuyên gia bảo mật duy trì kỹ năng của họ và nâng cao kỹ năng và kiến thức của những người khác. Một xem xét bổ sung là quy định này yêu cầu

rằng các cá nhân đảm bảo không ảnh hưởng tiêu cực đến nghề bảo vệ bằng cách liên kết chuyên nghiệp với những người có thể gây hại cho nghề.

Organizational Code of Ethics

Quy tắc đạo đức của tổ chức dựa trên sự an toàn của khối thịnh vượng chung và nghĩa vụ đối với các hiệu trưởng, chẳng hạn như người sử dụng lao động, nhà thầu và người lao động chuyên nghiệp. Nó đòi hỏi các chuyên gia phải tuân thủ và được coi là tuân thủ các tiêu chuẩn đạo đức cao nhất về hành vi.

Security Policies & Standards

Tất cả các chính sách, tiêu chuẩn, nguyên tắc và thủ tục đều hơi khác nhau, nhưng chúng cũng tương tác với nhau theo nhiều cách khác nhau. Ứng viên CISSP có nhiệm vụ nghiên cứu những khác biệt và mối quan hệ này và nhận ra các loại chính sách khác nhau và ứng dụng của chúng. Để phát triển và thực hiện thành công các chính sách, tiêu chuẩn, hướng dẫn và thủ tục về an toàn thông tin, điều quan trọng là phải đảm bảo rằng các nỗ lực của họ nhất quán với sứ mệnh, mục tiêu và mục tiêu của tổ chức.

Policy

Chính sách bảo mật là nền tảng của chương trình bảo mật thông tin của tổ chức. Chính sách bảo mật là một tuyên bố chính thức về các quy tắc mà những người được cấp quyền truy cập vào tài sản thông tin và công nghệ của tổ chức phải chấp nhận.

Bốn loại chính sách chính là

1. **Senior Management:** Một tuyên bố quản lý cấp cao về các mục tiêu an ninh của tổ chức, trách nhiệm của tổ chức và cá nhân, đạo đức và niềm tin cũng như các yêu cầu và kiểm soát chung.
2. **Regulatory**: Các chính sách ngắn gọn và chi tiết cao thường được yêu cầu bởi liên bang, tiểu bang, ngành hoặc các yêu cầu pháp lý khác.
3. **Advisory:** Không bắt buộc, nhưng rất khuyến khích, thường có các hình phạt cụ thể hoặc hậu quả nếu không tuân thủ. Hầu hết các chính sách thuộc loại này.
4. **Informative:** Chỉ thông báo, không có yêu cầu rõ ràng về sự tuân thủ. Các tiêu chuẩn, hướng dẫn và thủ tục là các yếu tố hỗ trợ của chính sách và cung cấp các chi tiết thực hiện cụ thể của chính sách.

Các tiêu chuẩn, hướng dẫn và thủ tục là các yếu tố hỗ trợ của chính sách và cung cấp các chi tiết thực hiện rõ ràng của chính sách.

Standards

Các tiêu chuẩn bảo mật cung cấp các tuyên bố theo quy định, các mục tiêu kiểm soát và các biện pháp kiểm soát để thực thi các chính sách bảo mật. Chúng có thể được phát triển nội bộ bởi tổ chức và được xuất bản bởi các cơ quan tiêu chuẩn, chẳng hạn như Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST), Tổ chức Tiêu chuẩn Quốc tế (ISO), hoặc các cơ quan tiêu chuẩn của từng quốc gia cụ thể.

Guidelines

Các hướng dẫn tương tự như các tiêu chuẩn, nhưng chúng hoạt động như các khuyến nghị chứ không phải là các yêu cầu bắt buộc. Nguyên tắc bảo mật cung cấp các phương pháp thực hành tốt nhất để hỗ trợ lựa chọn và triển khai các biện pháp kiểm soát bảo mật. Chúng có thể được sử dụng toàn bộ hoặc một phần trong khi thực hiện các tiêu chuẩn bảo mật.

Procedures

Các thủ tục cung cấp hướng dẫn chi tiết về cách thực hiện các chính sách cụ thể và đáp ứng các tiêu chí được xác định trong tiêu chuẩn. Các thủ tục bảo mật là các hướng dẫn có hệ thống để thực hiện các chính sách và tiêu chuẩn bảo mật.

Business Continuity Requirements

Các yêu cầu về tính liên tục của doanh nghiệp dựa trên việc lập kế hoạch liên tục trong kinh doanh (BCP) nhằm đảm bảo tính liên tục của các hoạt động CNTT được duy trì từ các địa điểm chính hoặc thay thế khi có sự cố hoặc các sự kiện thảm khốc. Trong các cấp độ bảo mật hoạt động này, bảo trì là một vấn đề quan trọng cần xem xét.

Develop and Document Scope and Plan

Business Continuity Planning (BCP)

BCP là một quá trình chủ động giải quyết việc tiếp tục hoạt động kinh doanh trong và sau dư chấn của các sự kiện gián đoạn như vậy. BCP nhằm mục đích ngăn chặn sự gián đoạn hoạt động.

Lập kế hoạch kinh doanh liên tục cho phép một tổ chức:

- Cung cấp phản ứng tức thì và thích hợp cho các tình huống khẩn cấp
- Bảo vệ tính mạng và đảm bảo an toàn
- Giảm tác động kinh doanh
- Tiếp tục các chức năng kinh doanh quan trọng
- Làm việc với các nhà cung cấp và đối tác bên ngoài trong thời gian khôi phục
- Giảm sự nhầm lẫn trong cuộc khủng hoảng
- Đảm bảo khả năng tồn tại của doanh nghiệp
- Nhanh chóng “thiết lập và chạy” sau thảm họa

BCP goals and objectives

BCP đòi hỏi những nỗ lực tương ứng của một nhóm nhân sự được rút ra từ các chức năng kinh doanh khác nhau của một tổ chức. Hãy để Chúng ta nhanh chóng xem xét mục tiêu và các mục tiêu được đề cập đến trong quá trình BCP.

Goals

- Mục tiêu của BCP là đảm bảo tính liên tục của hoạt động kinh doanh mà không ảnh hưởng đến toàn bộ tổ chức.
- Trong quá trình thiết kế BCP, tính sẵn có nên được coi là yếu tố quan trọng nhất.

Objectives

- An toàn tính mạng hoặc ngăn ngừa thiệt hại về người là một trong những mục tiêu chính của BCP.

- Một mục tiêu quan trọng khác của BCP là tránh bất kỳ thiệt hại nghiêm trọng nào đối với

kinh doanh.

BCP process

BCP bao gồm các bước sau. Các bước đơn giản hóa này tạo thành một mô hình vòng đời cho quy trình BCP:

1. **Scoping**

   Xác định phạm vi là một hoạt động rất quan trọng trong quy trình BCP. Phạm vi của BCP chủ yếu tập trung vào một quy trình kinh doanh. Xác định phạm vi bằng cách tập trung vào một quy trình kinh doanh, chúng ta sẽ có thể thấy một liên kết đầu cuối của tất cả các tài sản, hoạt động và quy trình liên quan. Do đó, nguyên tắc cơ bản của việc xác định phạm vi BCP là đảm bảo rằng nó phù hợp, có nghĩa là đảm bảo rằng quá trình xác định phạm vi bao gồm tất cả các nguồn lực thiết yếu.

2. **Initiating the Planning Process**

   Quá trình Lập kế hoạch Liên tục trong Kinh doanh được bắt đầu bằng cách thiết lập vai trò và trách nhiệm của các nhân sự liên quan.

3. **Performing Business Impact Analysis (BIA)**

   BIA là một loại ứng dụng đánh giá rủi ro nhằm đánh giá các tác động định tính và định lượng đối với hoạt động kinh doanh do một sự kiện gián đoạn. Các tác động định tính nói chung là các tác động hoạt động như không có khả năng cung cấp, trong khi các tác động định lượng liên quan đến tổn thất tài chính.

4. **Developing the BCP**

   Kế hoạch liên tục trong kinh doanh là các biện pháp chủ động xác định các quy trình kinh doanh quan trọng cần thiết cho tính liên tục và bền vững của doanh nghiệp dựa trên BIA.

5. **BC plan implementation**

   Quản lý cấp cao phải phê duyệt các kế hoạch kinh doanh liên tục được lập thành văn bản thích hợp và khi được phê duyệt, các kế hoạch được thực hiện.

6. **BC plan maintenance**

   Vòng đời BCP cũng bao gồm việc duy trì các kế hoạch. Các kế hoạch cần được đánh giá và cập nhật định kỳ dựa trên những thay đổi về kinh doanh, thay đổi công nghệ và thay đổi chính sách.

Business Impact Analysis (BIA)

Phân tích tác động kinh doanh (BIA) được coi là một phân tích chức năng, trong đó nhóm

thu thập dữ liệu thông qua các cuộc phỏng vấn và các nguồn tài liệu; tài liệu các chức năng kinh doanh, hoạt động và giao dịch; phát triển một hệ thống phân cấp các chức năng kinh doanh và cuối cùng áp dụng một sơ đồ phân loại để chỉ ra mức độ quan trọng của từng chức năng.

Business Impact Analysis Steps

Phân tích tác động kinh doanh theo các bước sau:

1. Lựa chọn các cá nhân để phỏng vấn để thu thập dữ liệu.
2. Tạo ra các kỹ thuật thu thập dữ liệu, chẳng hạn như khảo sát, bảng câu hỏi, phương pháp tiếp cận định tính và định lượng.
3. Xác định các chức năng kinh doanh quan trọng của công ty.
4. Xác định các nguồn lực mà các chức năng này phụ thuộc vào.
5. Tính toán xem các chức năng này có thể tồn tại trong bao lâu nếu không có các tài nguyên này.
6. Xác định các lỗ hổng và mối đe dọa đối với các chức năng này.
7. Tính toán rủi ro cho từng chức năng kinh doanh khác nhau.
8. Tài liệu phát hiện và báo cáo chúng cho ban giám đốc.

Personnel Security

Chính sách bảo mật nhân sự liên quan đến những người có liên quan đến tổ chức, chẳng hạn như nhân viên, nhà thầu, nhà tư vấn và người dùng.

Các chính sách này liên quan đến những điều sau:

- Các quy trình sàng lọc để xác thực các yêu cầu bảo mật
- Hiểu trách nhiệm bảo mật của họ
- Hiểu sự phù hợp của chúng với các vai trò bảo mật
- Giảm nguy cơ trộm cắp, gian lận hoặc sử dụng sai cơ sở vật chất

Candidate Screening and Hiring

Kiểm tra xác minh lý lịch chủ yếu được sử dụng trong quá trình sàng lọc ứng viên tuyển dụng.

Chúng có thể bao gồm những điều sau:

- Tham chiếu nhân vật để đánh giá các đặc điểm cá nhân của người nộp đơn. Các nguyên tắc về phương pháp hay nhất chỉ ra các tham chiếu ký tự từ ít nhất hai thực thể, chẳng hạn như từ doanh nghiệp và cá nhân.
- Tính đầy đủ và chính xác của sơ yếu lý lịch của người nộp đơn và việc xác minh các bằng cấp học tập và chuyên môn đã được tuyên bố là những bước kiểm tra quan trọng trong quá trình sàng lọc.
- Kiểm tra danh tính bằng cách xác minh tài liệu nhận dạng.
- Kiểm tra hồ sơ tội phạm cũng như kiểm tra tín dụng.

Employment Agreements and Policies

Các thỏa thuận lao động khác nhau nên được ký kết khi một cá nhân gia nhập một tổ chức hoặc được thăng chức lên một vị trí nhạy cảm hơn trong một tổ chức. Các thỏa thuận lao động thông thường bao gồm các thỏa thuận không cạnh tranh / không tiết lộ và các chính sách sử dụng được chấp nhận.

Onboarding and Termination Processes

Các quy trình gia nhập và kết thúc nên được chính thức hóa trong một tổ chức để đảm bảo đối xử công bằng và thống nhất và để bảo vệ tổ chức và tài sản thông tin của tổ chức.

Các phương pháp gia nhập tiêu chuẩn nên bao gồm kiểm tra lý lịch và các thỏa thuận tuyển dụng, cũng như quy trình huấn luyện và định hướng chính thức. Quá trình này có thể bao gồm giới thiệu chính thức cho các nhân sự chủ chốt của tổ chức, tạo tài khoản người dùng và chỉ định tài nguyên CNTT, chỉ định huy hiệu bảo mật và giấy phép đỗ xe và thảo luận chính sách chung với nhân viên Bộ phận Nhân sự.

Các thủ tục chấm dứt chính thức nên được thực hiện để giúp bảo vệ tổ chức khỏi các vụ kiện tiềm tàng, trộm cắp tài sản, phá hủy, truy cập trái phép hoặc bạo lực tại nơi làm việc. Các thủ tục nên được phát triển cho các tình huống khác nhau bao gồm từ chức, chấm dứt hợp đồng, sa thải, tai nạn hoặc tử vong, khởi hành ngay lập tức chống lại thông báo trước và các tình huống thù địch. Các thủ tục có thể bao gồm việc chấm dứt trách nhiệm, trả lại tài sản, xóa bỏ quyền truy cập, v.v.

The vendor, Consultant, and Contractor Agreements and Controls

Người dùng bên thứ ba, chẳng hạn như nhà cung cấp, nhà tư vấn và nhà thầu, cần quyền truy cập vào thông tin và các hệ thống liên quan dựa trên chức năng công việc. Bảo vệ thông tin bắt đầu với quy trình sàng lọc, bảo mật và các thỏa thuận không tiết lộ.

Compliance and Privacy Policy Requirements

Việc tuân thủ các chính sách, thủ tục, thực hiện các chức năng công việc một cách hợp pháp, các yêu cầu quy định và tuân thủ các cơ chế bảo vệ quyền riêng tư, được áp dụng trên phạm vi toàn diện trong một tổ chức.

Risk Management

Identification of Vulnerability & Threats

Vulnerability

A vulnerability là một điểm yếu trong hệ thống hoặc thiết kế của nó. The vulnerability có thể hiện diện ở bất kỳ cấp độ nào của kiến trúc hệ thống.

Classifying vulnerabilities giúp xác định tác động của nó đối với hệ thống. Cisco và các nhà cung cấp bảo mật khác đã tạo cơ sở dữ liệu được gọi là **The Common Vulnerabilitiesand Exposures (CVE)** phân loại các mối đe dọa qua internet. Nó có thể được tìm kiếm thông qua bất kỳ công cụ tìm kiếm nào hiện có. Sau đây là một số lý do quan trọng khiến lỗ hổng bảo mật có thể tồn tại trong hệ thống:

- Sai sót về chính sách
- Lỗi thiết kế
- Điểm yếu của giao thức
- Định cấu hình sai
- Lỗ hổng phần mềm
- Yếu tố con người
- Phần mềm độc hại
- Lỗ hổng phần cứng
- Quyền truy cập vật lý vào tài nguyên mạng.

Lỗ hổng bảo mật là một trong những thành phần chính, dẫn đến rủi ro đối với tài sản của tổ chức. Lỗ hổng bảo mật là điểm yếu của hệ thống, mạng, phần mềm, quy trình hoặc giao thức. Các lỗ hổng là điểm yếu bên trong, được khai thác nếu các biện pháp đối phó không được ngụ ý.

Threat

Mối đe dọa là khả năng xảy ra một cuộc tấn công. Các mối đe dọa có thể là kết quả của việc tiết lộ bất kỳ lỗ hổng nào trong hệ thống. Cấu hình biện pháp đối phó với các lỗ hổng bảo mật làm giảm các mối đe dọa đối với hệ thống.

A **threat** là bất kỳ mối nguy hiểm tiềm tàng nào đối với một tài sản. Sự hiện diện của một lỗ hổng trong hệ thống dẫn đến một mối đe dọa. Ai đó có thể tấn công hệ thống bằng cách lợi dụng các lỗ hổng và có thể truy cập thành công thông tin nhạy cảm hoặc xâm phạm các chính sách bảo mật và tiếp cận các tài sản có giá trị. Thực thể sử dụng lỗ hổng của hệ thống được gọi là **malicious actor** và đường dẫn được thực thể này sử dụng để khởi động một cuộc tấn công được gọi là

threat vector.

Risk Assessment

Nếu lỗ hổng và khả năng bị tấn công gặp nhau, nó sẽ dẫn đến rủi ro cho tài sản. Nếu có điểm yếu nhưng không có mối đe dọa, rủi ro đối với doanh nghiệp. Tương tự, một mối đe dọa không có bất kỳ lỗ hổng liên quan nào không tạo ra bất kỳ rủi ro nào. Xác định mức độ rủi ro là quá trình định lượng khả năng xảy ra mối đe dọa & ảnh hưởng của nó đối với doanh nghiệp.

Phân tích rủi ro là một quá trình đánh giá rủi ro, cho phép chuyên gia bảo mật xác định và lập danh mục các rủi ro khác nhau. Quản lý rủi ro xác định mức độ mà một tổ chức có thể chấp nhận sự không chắc chắn. Sự không chắc chắn này có thể ở dạng rủi ro hoặc cơ hội. Về khả năng, cả hai trường hợp đều có thể ảnh hưởng đến tổ chức. Phân tích và quản lý rủi ro có thể giúp các chuyên gia bảo mật liên kết với một tổ chức xây dựng một kế hoạch và kỹ thuật nhất định để đối phó với những bất ổn này.

Enterprise Risk Management

Quy trình Quản lý Rủi ro Doanh nghiệp của NIST bao gồm các bước sau:

- **Categorize** hệ thống thông tin (mức độ quan trọng / độ nhạy cảm)
- **Select** và điều chỉnh các biện pháp kiểm soát an ninh cơ bản (tối thiểu)
- **Supplement** kiểm soát an ninh dựa trên đánh giá rủi ro
- **Document** kiểm soát an ninh trong kế hoạch bảo mật hệ thống
- **Implement** kiểm soát an ninh trong hệ thống thông tin
- **Assess** kiểm soát an ninh cho hiệu quả
- **Authorize** vận hành hệ thống thông tin dựa trên rủi ro nhiệm vụ
- **Monitor** kiểm soát an ninh trên cơ sở liên tục

Applicable types of controls

Các biện pháp kiểm soát này bao gồm các kế hoạch và phương pháp phối hợp, được áp dụng trong một tổ chức để bảo vệ tài sản của họ. Các biện pháp kiểm soát này kiểm tra tính chính xác, độ tin cậy và hiệu quả của các chính sách quản lý. Ba loại điều khiển như sau:

1. Kiểm soát Phòng ngừa
2. Kiểm soát thám tử
3. Kiểm soát sửa chữa

Preventive

Kiểm soát Phòng ngừa là kiểm soát được thiết kế cho các phương tiện phòng ngừa. Đây là sự kiểm soát chủ động, đảm bảo rằng các mục tiêu đang được đáp ứng. Ví dụ, việc tách biệt các nhiệm vụ làm giảm nguy cơ xảy ra các sự cố không phù hợp và bất thường bằng cách thực hiện một nhiệm vụ nhất định giữa những người khác nhau. Việc chia quy trình giao dịch thanh toán thành ba bước giúp giảm thiểu khả năng xảy ra sai sót. Ủy quyền / phê duyệt trong đó một số người chịu trách nhiệm phê duyệt giao dịch. Một cá nhân chịu trách nhiệm kế toán và người khác chịu trách nhiệm thanh toán để giảm khả năng xảy ra sai sót trong quá trình.

Detective

Kiểm soát Thám tử là kiểm soát được thiết kế để khắc phục sự cố hoặc xác định các lỗi, sự cố và bất thường. Các biện pháp kiểm soát này có hiệu lực sau một sự cố. Ví dụ về kiểm soát của thám tử có thể là quy trình khắc phục sự cố, xem xét hoạt động, đối chiếu hoặc kiểm toán.

Corrective

Kiểm soát sửa chữa là các kiểm soát được thực hiện như một phản ứng với các kiểm soát của thám tử. Khi xử lý sự cố, đánh giá hoặc kiểm tra quy trình kiểm soát của thám tử để tìm ra bất kỳ lỗ hổng nào hoặc bất kỳ hoạt động khai thác nào kích hoạt nó, kiểm soát khắc phục sẽ đảm bảo và giảm tác động của nó. Nó cũng bao gồm việc thực thi các chính sách để khôi phục một hệ thống hoạt động bình thường.

Security Control Assessment (SCA)

Đánh giá Kiểm soát An ninh là một nguyên tắc đảm bảo rằng các chính sách an ninh được thực thi trong một tổ chức đang đáp ứng các mục tiêu và mục tiêu của họ. Đánh giá Kiểm soát An ninh đánh giá những người thực thi chính sách bảo mật này và chịu trách nhiệm về hệ thống thông tin nếu họ đang tuân thủ các mục tiêu bảo mật đã nêu. SCA đánh giá các biện pháp kiểm soát an ninh có thể quản lý, vận hành và kỹ thuật trong một hệ thống thông tin để xác định việc thực thi chính xác và hiệu quả các biện pháp kiểm soát này.

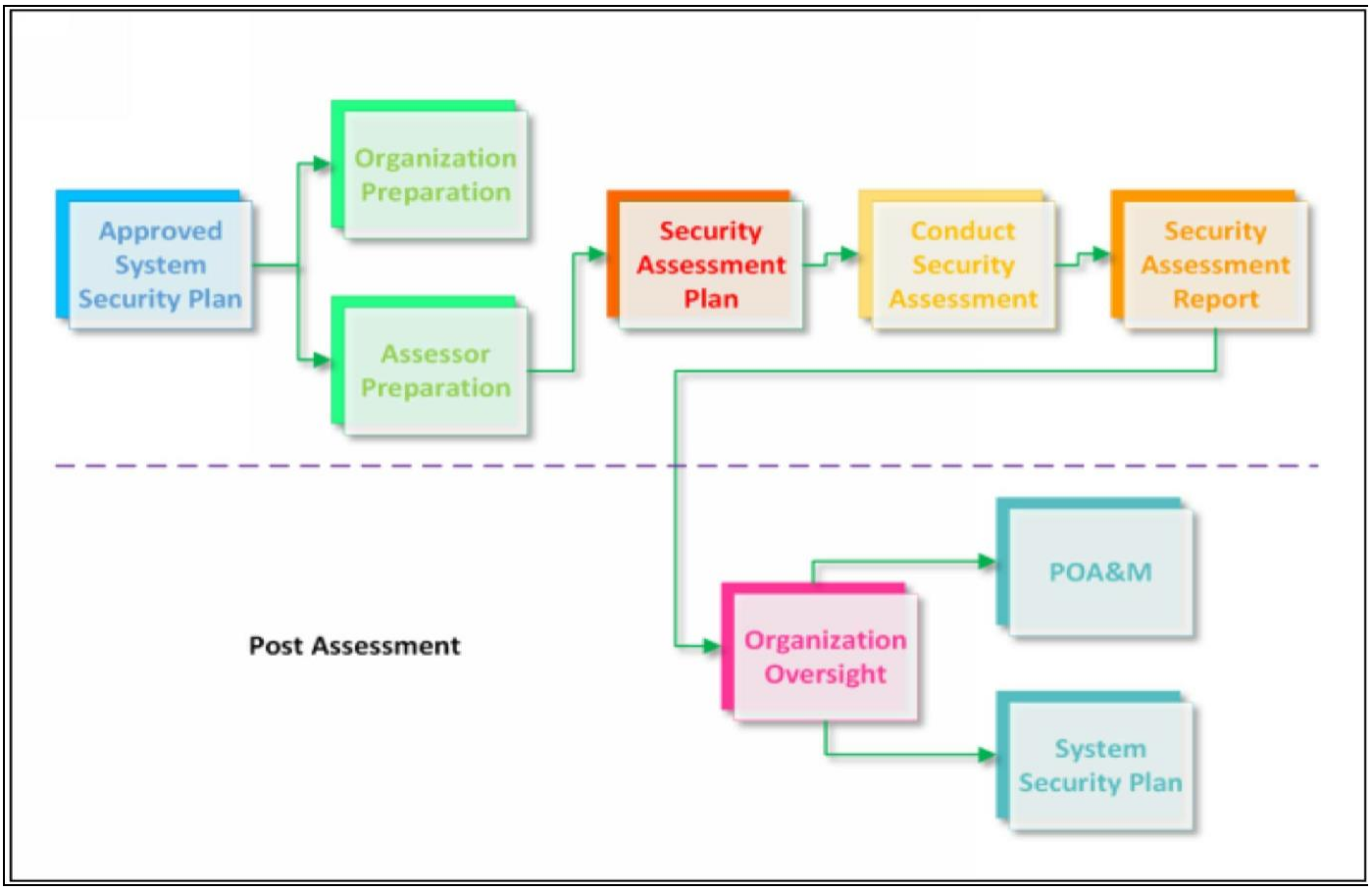


Figure 3. NIST-Security Control Assessment Framework

Kết quả Đánh giá Kiểm soát An ninh cung cấp sự chắc chắn hoặc bằng chứng về việc thực thi kiểm soát an ninh trong một tổ chức cũng như tính hiệu quả của nó đối với hệ thống của tổ chức. CSA cũng báo cáo về chất lượng của các quy trình quản lý rủi ro bao gồm các kế hoạch hành động ứng phó sự cố.

Báo cáo CSA rất quan trọng. Kết quả từ quá trình CSA giúp xác định

hiệu quả tổng thể, độ tin cậy và sức mạnh của các biện pháp kiểm soát an ninh liên quan đến một tổ chức. Quy trình đánh giá kiểm soát an ninh được thực hiện tốt sẽ cung cấp các yếu tố đầu vào để tăng cường kiểm soát an ninh đang hoạt động, xác định điểm yếu và điểm mạnh của các biện pháp kiểm soát, đồng thời tạo điều kiện cho một giải pháp tiếp cận hiệu quả về chi phí.

Asset valuation

Mọi thông tin đều có giá trị. Thông tin hoặc tài sản nhạy cảm và quan trọng có giá trị hơn các tài nguyên không quan trọng. Giá trị của tài sản được tính dưới dạng chi phí hoặc giá trị cảm nhận của nó đối với một tổ chức, bên trong hoặc bên ngoài.

Methods of Valuation

Có hai loại phương pháp xác định giá trị thông tin, như sau:

1. **Subjective Method**

   Theo lý thuyết chủ quan về giá trị, giá trị của một tài sản được xác định bởi các hành động quan trọng của cá nhân đặt lên nó. Các phương pháp chủ quan bao gồm việc tạo, phổ biến và thu thập dữ liệu từ danh sách kiểm tra hoặc khảo sát.

2. **Objective Method**

   Định giá khách quan là một thước đo hoặc thước đo thống kê, có thể cung cấp một cái nhìn khách quan về định giá thông tin. Chúng dựa trên các phép đo định lượng cụ thể thay vì định tính.

Tangible Asset Valuation

Tài sản hữu hình là tài sản vật chất; do đó, những tài sản này được định giá bằng cách trừ khấu hao khỏi nguyên giá. Với mục đích đánh giá, các chuyên gia an toàn thông tin phải biết nguyên giá thực tế của các tài sản này để ước tính giá trị tài sản một cách chính xác. Tương tự, một số giá trị tài sản này có thể thay đổi tùy theo nhu cầu và giá trị thị trường.

Các thông số sau được coi là để ước tính giá trị của tài sản hữu hình:

- Chi phí thực
- Khấu hao
- Giá trị thị trường / Giá trị
- So sánh chi phí thay thế
- Chi phí cạnh tranh cho một tài sản liên quan đến khả năng

Intangible Asset Valuation

Do đó, tài sản vô hình không phải là tài sản vật chất, những loại tài sản này được phân loại là xác định

và tài sản vô hình vô thời hạn.

1. **Definite Intangible Assets**

   Tài sản vô hình có một số thời hạn sử dụng. Những tài sản này mất đi tầm quan trọng và giá trị khi bằng sáng chế hết hạn.

2. **Indefinite Intangible Assets**

   Nội dung có thời hạn sử dụng không xác định.

Đối với một người nào đó để ước tính giá trị của một tài sản vô hình, các phương pháp sau đây thường được coi là có thể chấp nhận được

- Chi phí để tạo và thay thế tài sản
- Viết hoa lợi nhuận trước đây
- Tránh hoặc tiết kiệm chi phí

Reporting

Trong môi trường an toàn thông tin, chuyên gia bảo mật phải duy trì tài liệu và báo cáo thích hợp về từng sự kiện và sự cố để duy trì khả năng hiển thị. Các báo cáo này không chỉ giúp họ mà còn giúp các cơ quan hữu quan giám sát, lập kế hoạch và thực hiện các hành động cần thiết. Báo cáo là một phần quan trọng của bảo mật thông tin vì nó giúp khắc phục các nguyên nhân gốc rễ, sơ hở và tiết kiệm thời gian khi các điều kiện tương tự được đáp ứng trong tương lai. Báo cáo có thể là kỹ thuật hoặc phi kỹ thuật. Nếu chúng ta tập trung vào các báo cáo kỹ thuật, có nhiều loại báo cáo khác nhau được tạo ra ở các điều kiện khác nhau tùy theo yêu cầu. Báo cáo sự cố là tập hợp các dữ kiện và số liệu của một sự cố cụ thể với đề xuất các biện pháp đối phó và ứng phó sự cố. Báo cáo kiểm toán, Báo cáo kinh doanh, Báo cáo quản lý rủi ro và các báo cáo khác là các ví dụ về báo cáo.

Tương tự, trong khi kiểm toán bảo mật, đánh giá lỗ hổng và kiểm tra thâm nhập, báo cáo đóng một vai trò quan trọng. Cần có báo cáo và tài liệu để kiểm tra trong tương lai. Các báo cáo này giúp xác định các lỗ hổng trong giai đoạn mua lại. Kiểm toán và Thâm nhập cũng yêu cầu các báo cáo đã thu thập trước đó. Khi bất kỳ sửa đổi nào trong cơ chế bảo mật được yêu cầu, các báo cáo này sẽ giúp thiết kế cơ sở hạ tầng bảo mật. Cơ sở dữ liệu trung tâm thường giữ các báo cáo này.

Các báo cáo chứa:

- Nhiệm vụ được thực hiện bởi mỗi thành viên trong nhóm.
- Phương pháp & công cụ được sử dụng.
- Kết quả.

- Khuyến nghị.
- Thông tin thu thập từ các giai đoạn khác nhau.

Ngoài lợi thế kỹ thuật và tầm quan trọng của báo cáo, báo cáo còn thiết lập mối quan hệ kinh doanh chuyên nghiệp, đáng tin cậy giữa các nhà điều hành kinh doanh, ban quản lý và người dùng cuối..

Risk Management Framework (RMF)

Khung quản lý rủi ro (RMF) là một khuôn khổ bảo mật thông tin. Các mục tiêu của RMF như sau:

- Để cải thiện bảo mật thông tin
- Để tăng cường các quy trình quản lý rủi ro
- Để khuyến khích sự có đi có lại giữa các cơ quan liên bang

RMF chuyển đổi hiệu quả các chương trình Chứng nhận và Công nhận (C&A) truyền thống thành một quy trình vòng đời sáu bước bao gồm:

1. Phân loại hệ thống thông tin
2. Lựa chọn các biện pháp kiểm soát an ninh
3. Thực hiện các biện pháp kiểm soát an ninh
4. Đánh giá các biện pháp kiểm soát an ninh
5. Ủy quyền hệ thống thông tin
6. Giám sát các biện pháp kiểm soát an ninh

Figure 4. NIST-Risk Management Framework

Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) đã xây dựng hướng dẫn chi tiết về việc triển khai RMF với sự hợp tác của Tổ chức Sáng kiến Chuyển đổi Lực lượng Đặc nhiệm Chung (JTFTI).

Risk Management Framework (RMF)	Description
NIST Special Publication (SP)	Contains detailed guidance on the RMF roles, responsibilities, and the life-

800-37 (Rev. 1)	cycle process.
Federal Information Processing Standard (FIPS) Publication 199	
NIST SP 800-60 vol. 1 , NIST SP 800-60 vol. 2	
FIPS 200 and NIST SP 800-53 (Rev. 4)	Contain details on the security controls (requirements) for federal information systems
NIST SP 800-53A (Rev. 1)	Contains guidance on security controls assessment
NIST SP 800-137	Contains guidance on security controls monitoring

Table 1-02: Risk Management Framework

Threat Modeling

Mô hình mối đe dọa là một mô hình phân loại, mô tả các mối đe dọa đối với một tổ chức, tại sao và làm thế nào những mối đe dọa này trở nên dễ bị tổn thương. Với mô hình mối đe dọa, bạn có thể xác định những kẻ tấn công và đánh giá mục tiêu của chúng. Hơn nữa, nó cũng giúp khám phá các kỹ thuật khai thác tiềm năng. Mô hình hóa mối đe dọa cũng giúp khám phá các mối đe dọa tập trung vào thiết kế hệ thống và mạng bao gồm từng thành phần.

Ngoài Hệ thống và Mạng, là một phần của giai đoạn thiết kế và phát triển của Vòng đời phát triển phần mềm (SDLC), mô hình hóa mối đe dọa cũng giúp các kiến trúc sư thiết kế xác định các mối đe dọa, các vấn đề bảo mật tiềm ẩn và lỗ hổng bảo mật. Việc tối ưu hóa này giúp giải quyết các vấn đề một cách hiệu quả và tiết kiệm chi phí.

Threat Modeling Concept

Thông thường, quy trình lập mô hình Đe dọa bao gồm một số bước cơ bản bao gồm xác định các mục tiêu, mối đe dọa và tính dễ bị tổn thương liên quan với các mục tiêu đó và sau đó xác định các biện pháp phòng ngừa, biện pháp đối phó và kỹ thuật giảm thiểu. Sau đây là các bước của quy trình lập mô hình Đe doạ:

1. Xác định khách quan & phạm vi đánh giá
2. Xác định các tác nhân đe dọa và các cuộc tấn công có thể xảy ra
3. Hiểu các biện pháp đối phó hiện có
4. Xác định các lỗ hổng có thể khai thác
5. Các rủi ro đã xác định được ưu tiên
6. Xác định các biện pháp đối phó để giảm bớt các mối đe dọa

Threat Modeling Process

Mô hình hóa mối đe dọa là một cách tiếp cận để xác định, chẩn đoán và hỗ trợ với các mối đe dọa và lỗ hổng bảo mật của hệ thống. Đây là một cách tiếp cận để quản lý rủi ro, chuyên biệt tập trung vào việc phân tích bảo mật hệ thống và bảo mật ứng dụng chống lại các mục tiêu bảo mật. Việc xác định các mối đe dọa và rủi ro này giúp tập trung và hành động vào một sự kiện để đạt được mục tiêu. Thu thập dữ liệu của một tổ chức, thực hiện các quy trình xác định và đánh giá thông tin thu được để phân tích thông tin có thể ảnh hưởng đến bảo mật của ứng dụng. Tổng quan về ứng dụng bao gồm quá trình xác định ứng dụng để xác định ranh giới tin cậy và luồng dữ liệu. Việc phân rã ứng dụng và xác định mối đe dọa đã giúp xem xét chi tiết các mối đe dọa và xác định mối đe dọa đang vi phạm kiểm soát an ninh. Việc xác định và xem xét chi tiết mọi khía cạnh này cho thấy các lỗ hổng và điểm yếu của môi trường an toàn thông tin.

Hầu hết các phương pháp luận về mô hình mối đe dọa đều trả lời một hoặc

- nhiều câu hỏi sau:

- Chúng ta đang xây dựng cái gì?
- Cái mà có thể sai lầm?
- Chúng ta sẽ làm gì về điều đó?
- Chúng ta đã làm tốt công việc chưa?

Threat Modeling Tools

Vendor	Threat Modeling Tool
Microsoft	Threat Modeling Tool
MyAppSecurity	Threat Modeler
IriusRisk	Threat Modeling Tool
Scandinavian	securiCAD
Security Compass	SD Elements

Table 1-03: Threat Modeling Tools

Threat Modeling Methodologies

Có các lựa chọn khác nhau để thực hiện các phương pháp lập mô hình mối đe dọa. Bốn phương pháp được thảo luận dưới đây là phương pháp nổi tiếng nhất.

STRIDE Methodology

STRIDE là một phương pháp lập mô hình mối đe dọa do Microsoft phát triển, tập trung vào các mối đe dọa bảo mật máy tính. Nó là một cách ghi nhớ đối với các mối đe dọa bảo mật gồm sáu loại, như sau:

- Giả mạo
- Tampering
- Thoái thác
- Công bố thông tin

- Từ chối dịch vụ (DoS)
  Nâng cao đặc quyền

Process for Attack Simulation and Threat Analysis (PASTA)

PASTA là một phương pháp lấy rủi ro làm trung tâm. Quy trình bảy bước của PASTA cung cấp sự phù hợp của các mục tiêu và yêu cầu kinh doanh, các vấn đề tuân thủ và phân tích. Phương pháp luận này tập trung vào quá trình xác định, liệt kê và cho điểm các mối đe dọa động. Khi quá trình mô hình hóa mối đe dọa sử dụng phương pháp PASTA được hoàn thành, nó mang đến một phân tích chi tiết về các mối đe dọa đã được xác định và cung cấp cái nhìn tập trung về các ứng dụng và cơ sở hạ tầng. Hình sau liệt kê bảy bước của phương pháp PASTA:

Figure 5. PASTA Methodology Steps

Trike Methodology

Trike là một phương pháp và công cụ lập mô hình mối đe dọa mã nguồn mở. Dự án bắt đầu vào năm 2006 như một nỗ lực nhằm nâng cao hiệu quả và hiệu quả của các phương pháp lập mô hình mối đe dọa hiện có và đang được tích cực sử dụng và phát triển.

Khung mô hình mối đe dọa Trike được sử dụng cho các quy trình kiểm tra bảo mật. Các mô hình đe dọa dựa trên "mô hình yêu cầu". Phân tích mô hình yêu cầu tạo ra một biểu mẫu mô hình mối đe dọa trong đó các mối đe dọa được liệt kê và ấn định các giá trị rủi ro.

VAST Methodology

VAST là viết tắt của mô hình Visual, Agile và Simple Threat. Đó là một cách tiếp cận mô hình mối đe dọa thực tế. Có hai loại mô hình mối đe dọa:

- Các mô hình mối đe dọa ứng dụng
- Các mô hình mối đe dọa hoạt động

Sự khác biệt đáng kể nhất trong phương pháp luận của VAST là khả năng cho phép các tổ chức mở rộng quy mô trên hàng nghìn mô hình mối đe dọa. Các trụ cột của quy trình có thể mở rộng, tự động hóa, tích hợp và cộng tác là nền tảng của VAST. Khi quy trình lập mô hình mối đe dọa của tổ chức trưởng thành, các trụ cột này cho phép tổ chức phát triển một phương pháp lập mô hình mối đe dọa tự phục vụ bền vững do các nhóm DevOps thúc đẩy thay vì nhóm bảo mật.

Application of Risk-based Management to Supply Chain

Trong các phần trước, chúng ta đã thảo luận về một số cân nhắc liên quan đến đánh giá rủi ro & quản lý rủi ro và kết nối kỹ thuật giữa hệ thống thông tin và bên thứ ba. Cần phải trao đổi thông tin giữa các nhân viên của một tổ chức và các bên thứ ba, một loại kết nối an toàn giữa họ và luồng dữ liệu được mã hóa là mối quan tâm cơ bản. Tuy nhiên, có nhiều mối quan tâm hơn liên quan đến việc quản lý rủi ro của bên thứ ba. Không một tổ chức nào có thể cung cấp hiệu quả tất cả các dịch vụ hành chính chỉ sử dụng nhân viên được tuyển dụng. Thuê ngoài và thỏa thuận hợp đồng với các tổ chức bên thứ ba là cách hiệu quả và hiệu quả để cung cấp một số dịch vụ quan trọng.

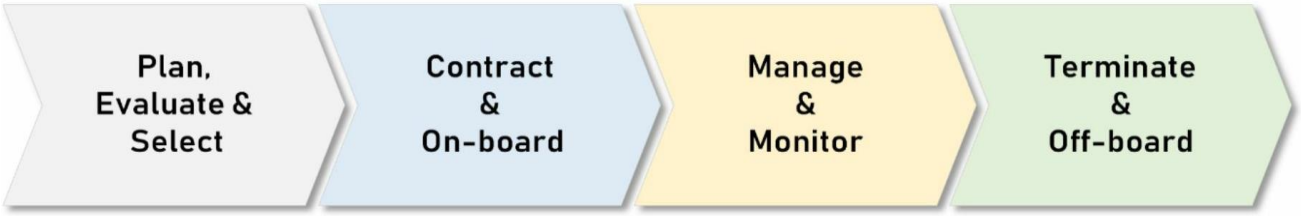


Figure 6. Third-Party Management Life-Cycle

Sau đây là một số bên thứ ba phổ biến, thường được tham gia với mọi tổ chức:

- Nhà cung cấp
- Các nhà cung cấp
- Khách hàng
- Người bán lại
- Chuyên gia tư vấn
- Nhà phân phối
- Người môi giới

Third-party assessment and monitoring

Khuôn khổ quản lý rủi ro của bên thứ ba dành cho bên thứ ba không khác với khuôn khổ quản lý rủi ro được sử dụng nội bộ trong một tổ chức. Có bên thứ ba

hợp đồng dẫn đến hiệu quả chi phí và kết quả không thiên vị. Cả tổ chức và bên thứ ba đều cần phải chuẩn bị và hiểu sâu sắc về vai trò, trách nhiệm và những hạn chế của họ. Với sự hợp tác, cả hai bên có thể đảm bảo năng suất hiệu quả. Các bên thứ ba nên hạn chế việc chia sẻ thông tin bí mật cho những người đã được xác định.

Key Challenges in Third-Party Risk Management

- Tăng độ phức tạp của mạng bên thứ ba và quản lý mạng đó
- Rủi ro không quản lý được việc tuân thủ quy định
- Chi phí bổ sung để giám sát bên thứ ba
- Thiếu sự hợp tác giữa các bên
- Rủi ro rò rỉ thông tin / dữ liệu

Minimum security requirements

Trước khi mua dịch vụ, có bất kỳ thỏa thuận nào hoặc bắt đầu bất kỳ quy trình nào với bên thứ ba, tổ chức phải đánh giá các tiêu chí, khả năng, vai trò, trách nhiệm, hạn chế và rủi ro của các bên thứ ba đã thỏa thuận.

- Người đánh giá của bên thứ ba phải được chứng nhận về Hệ thống quản lý an ninh thông tin (phù hợp với ISO / IEC 27001: 2005).
- Các bên thứ ba nên sẵn sàng tuân thủ các chính sách và thủ tục bảo mật của tổ chức.
- Bên thứ ba phải có nhân viên được chứng nhận trong các lĩnh vực an toàn thông tin (các tổ chức nên kiểm tra tính chính xác của trình độ chuyên môn của người đánh giá bên thứ ba).

Key Components of Third-Party Risk Management Framework

Sau đây là các thành phần chính của Khung quản lý rủi ro bên thứ ba (TPRM):

- Lập kế hoạch & định nghĩa quy trình
- Phân đoạn & Sàng lọc
- Trình độ chuyên môn
- Bảo mật & Quyền
- Quy trình làm việc
- Giảm thiểu rủi ro
- Giám sát liên tục
- Báo cáo & Trang tổng quan
- Kho lưu trữ tập trung
- Cảnh báo & Thông báo

Security Awareness, Education & Training

Nhận thức về bảo mật thường là một yếu tố không được chú ý trong một chương trình bảo mật thông tin. Mặc dù bảo mật là trọng tâm của các nhà bảo mật trong các chức năng hàng ngày của họ, nhưng người dùng phổ thông thường có cùng mức độ nhận thức về bảo mật này. Do đó, người dùng có thể vô tình trở thành mắt xích yếu nhất trong một chương trình bảo mật thông tin.

Ba thành phần chính của một chương trình nâng cao nhận thức về an ninh hiệu quả là chương trình nâng cao nhận thức chung, đào tạo chính thức và giáo dục.

Awareness

Chương trình nâng cao nhận thức về bảo mật chung cung cấp thông tin bảo mật cơ bản và đảm bảo rằng mọi người đều hiểu tầm quan trọng của bảo mật. Các chương trình nâng cao nhận thức có thể bao gồm các yếu tố sau:

- **Indoctrination and orientation:** Nhân viên và nhà thầu mới nên có kiến thức và định hướng cơ bản. Trong quá trình giảng dạy, họ có thể nhận được một bản sao của chính sách bảo mật thông tin của công ty, được yêu cầu xác nhận và ký các tuyên bố sử dụng được chấp nhận và các thỏa thuận không tiết lộ, đồng thời gặp gỡ người giám sát ngay lập tức và các thành viên thích hợp của đội bảo mật và nhân viên CNTT.
- **Presentations:** Các bài giảng, bài thuyết trình video và Đào tạo dựa trên máy tính tương tác (CBT) là những công cụ tuyệt vời để cung cấp thông tin và đào tạo bảo mật.
- **Printed materials:** Áp phích bảo mật, bản tin công ty và bản tin định kỳ rất hữu ích để phổ biến thông tin cơ bản như các mẹo bảo mật và nâng cao nhận thức về bảo mật.

Training

Các chương trình đào tạo chính thức cung cấp nhiều thông tin chi tiết hơn một chương trình nâng cao nhận thức có thể tập trung vào các kỹ năng hoặc nhiệm vụ liên quan đến bảo mật cụ thể.

Các chương trình đào tạo như vậy có thể bao gồm:

- **Classroom training:** Đào tạo có sự hướng dẫn của người hướng dẫn hoặc đào tạo được hỗ trợ chính thức khác, có thể tại trụ sở công ty hoặc cơ sở đào tạo của công ty
- **On-the-job training:** Có thể bao gồm cố vấn trực tiếp với đồng nghiệp hoặc người giám sát trực tiếp
- **Technical or vendor training:** Đào tạo về một sản phẩm hoặc công nghệ cụ thể do bên thứ ba cung cấp

- **Apprenticeship or qualification programs:** Tình trạng tập sự chính thức hoặc tiêu chuẩn trình độ chuyên môn phải được hoàn thành một cách thỏa đáng trong một khoảng thời gian nhất định.

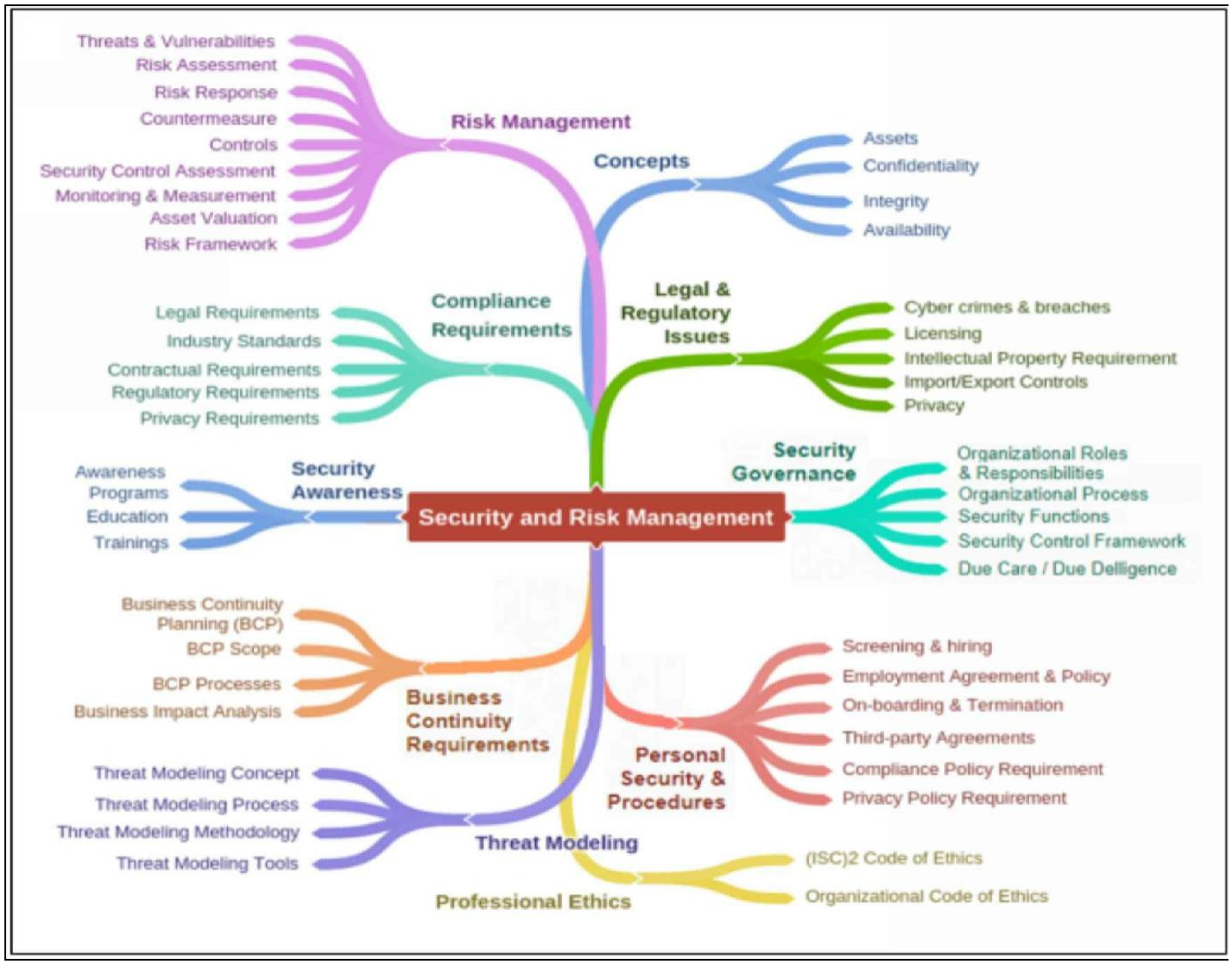
Education

Một chương trình giáo dục cung cấp mức đào tạo bảo mật sâu nhất, tập trung vào các nguyên tắc, phương pháp luận và khái niệm cơ bản.

Một chương trình giáo dục có thể bao gồm

- **Continuing education requirements:** Các Đơn vị Giáo dục Thường xuyên (CEU) đang trở nên phổ biến để duy trì các chứng chỉ chuyên môn hoặc kỹ thuật cấp cao như CISSP hoặc Chuyên gia Kết nối Internet được Chứng nhận của Cisco (CCIE).
- **Certificate programs:** Nhiều trường cao đẳng và đại học cung cấp các chương trình giáo dục dành cho người lớn có các lớp học về các môn học hiện tại và phù hợp cho các chuyên gia đang làm việc.
- **Formal education or degree requirements:** Nhiều công ty cung cấp hỗ trợ học phí hoặc học bổng cho nhân viên đăng ký các lớp học phù hợp với nghề nghiệp của họ.

Mind Map


Security and Risk Management
Risk Management
Threats & Vulnerabilities
Risk Assessment
Risk Response
Countermeasure
Controls
Security Control Assessment
Monitoring & Measurement
Asset Valuation
Risk Framework
Concepts
Assets
Confidentiality
Integrity
Availability
Compliance Requirements
Legal Requirements
Industry Standards
Contractual Requirements
Regulatory Requirements
Privacy Requirements
Legal & Regulatory Issues
Cyber crimes & breaches
Licensing
Intellectual Property Requirement
Import/Export Controls
Privacy
Security Awareness
Awareness Programs
Education
Trainings
Security Governance
Organizational Roles & Responsibilities
Organizational Process
Security Functions
Security Control Framework
Due Care / Due Delligence
Business Continuity Requirements
Business Continuity Planning (BCP)
BCP Scope
BCP Processes
Business Impact Analysis
Personal Security & Procedures
Screening & hiring
Employment Agreement & Policy
On-boarding & Termination
Third-party Agreements
Compliance Policy Requirement
Privacy Policy Requirement
Threat Modeling
Threat Modeling Concept
Threat Modeling Process
Threat Modeling Methodology
Threat Modeling Tools
Professional Ethics
(ISC)2 Code of Ethics
Organizational Code of Ethics

Practice Questions

1. Rủi ro nào sau đây liên quan đến tính bảo mật?
- **A.** Tiết lộ trái phép
- **B.** Sửa đổi dữ liệu
- **C.** Không có sẵn
- **D.** Từ chối

2. Khi hai tổ chức quyết định hợp nhất thành một tổ chức duy nhất, quá trình tổ chức này được gọi là:
- **A.** Mua lại
- **B.** Divestiture
- **C.** Gia công phần mềm
- **D.** Nâng cấp

3. Khi một bộ phận của tổ chức bị bán hoặc tách ra; quy trình tổ chức này được gọi là:
- **A.** Mua lại
- **B.** Divestiture
- **C.** Gia công phần mềm
- **D.** Nâng cấp

4. Ai chịu trách nhiệm giám sát, động viên và chỉ đạo các ủy ban an ninh.
- **A.** CSO
- **B.** Hội đồng quản trị
- **C.** Kiểm toán viên
- **D.** IAO

5. Ai chịu trách nhiệm bảo vệ tài sản thông tin?
- **A.** Giám đốc An ninh (CSO)
- **B.** Ủy ban An ninh (SC)
- **C.** Ủy ban An ninh Địa phương (LSC)
- **D.** Chủ sở hữu tài sản thông tin (IAO)

6. Khi người dùng được chuyển hướng đến một trang web độc hại do kẻ tấn công tạo ra; kiểu tấn công này được gọi là

A. Lừa đảo
B. Dược phẩm
C. Lừa đảo qua SMS
D. Theo dõi trên mạng

7. Khi người dùng bị dụ đến một kẻ tấn công đã xây dựng trang web bất hợp pháp trông giống với trang web thực mà người dùng dự định truy cập; kiểu tấn công này được gọi là

A. Lừa đảo
B. Dược phẩm
C. Lừa đảo qua SMS
D. Theo dõi trên mạng

8. Luồng dữ liệu Transborder được gọi là:

A. Dữ liệu xuyên biên giới quốc gia
B. Dữ liệu xuyên biên giới tổ chức
C. Dữ liệu trên các vùng mạng
D. Không có điều nào ở trên

9. Một biểu tượng hoặc nhãn hiệu duy nhất được sử dụng để đại diện cho sản phẩm của một cá nhân hoặc tổ chức được gọi là:

A. Bản quyền
B. Nhãn hiệu
C. Bằng sáng chế
D. Sở hữu trí tuệ

0. Một loại ứng dụng đánh giá rủi ro cố gắng đánh giá các tác động định tính và định lượng đối với hoạt động kinh doanh do một sự kiện gián đoạn được gọi là

A. Phân tích tác động kinh doanh (BIA)
B. Lập kế hoạch liên tục kinh doanh (BCP)
C. Phân tích rủi ro
D. Quản lý sự cố

1. Kiểm soát được thiết kế để khắc phục sự cố hoặc xác định lỗi, sự cố và bất thường được gọi là
   - **A.** Kiểm soát Phòng ngừa
   - **B.** Kiểm soát thám tử
   - **C.** Kiểm soát sửa chữa
   - **D.** Không có điều nào ở trên

2. Cơ quan chính nào đảm bảo rằng các chính sách bảo mật được thực thi trong một tổ chức đang đáp ứng các mục tiêu và mục tiêu của họ:
   - **A.** Đánh giá kiểm soát an ninh (SCA)
   - **B.** Đánh giá rủi ro
   - **C.** Kiểm tra thâm nhập
   - **D.** Kiểm toán

3. Tài sản vô hình trong hệ thống thông tin là:
   - **A.** Tài sản vật chất
   - **B.** Tài sản phi vật chất
   - **C.** Cả vật chất và phi vật chất
   - **D.** Không có điều nào ở trên

4. Công cụ nào sau đây là công cụ mô hình hóa mối đe dọa?
   - **A.** Phần tử SD
   - **B.** QRadar
   - **C.** Wireshark
   - **D.** Nessus

5. Phương pháp nào sau đây không phải là phương pháp luận mô hình hóa mối đe dọa?
   - **A.** STRIDE
   - **B.** PASTA
   - **C.** TRIKE
   - **D.** VAST
   - **E.** Không có điều nào ở trên

6. Phương pháp nào sau đây là phương pháp lập mô hình mối đe dọa của Microsoft?

A. STRIDE
B. PASTA
C. TRIKE
D. VAST
E. Không có điều nào ở trên

7. Bạn sẽ được thuê trong một ủy ban chịu trách nhiệm xác định phạm vi rủi ro, xem xét đánh giá rủi ro, báo cáo kiểm toán và phê duyệt các thay đổi quan trọng đối với các chính sách và chương trình bảo mật. Bạn sẽ tham gia ủy ban nào?

A. Ủy ban chính sách an ninh
B. Ủy ban kiểm toán
C. Ủy ban quản lý rủi ro
D. Ban chỉ đạo an ninh