**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**----------**

**PHẠM HOÀNG DUY**

**NGUYỄN NGỌC ĐIỆP**

# BÀI GIẢNG

# QUẢN LÝ AN TOÀN THÔNG TIN

**HÀ NỘI 2022**

# Lời nói đầu

Sự phát triển mạnh mẽ của công nghệ mạng Internet và sự phổ biến rộng rãi của các ứng dụng máy tính khiến cho việc đảm bảo an toàn thông tin trong các hoạt động thường xuyên của các cơ quan, tổ chức cũng như cá nhân được quan tâm và đầu tư nhiều công sức và tiền của. Quản lý an toàn thông tin là một trong những môn cơ sở quan trọng dành cho sinh viên năm thứ 3, chuyên ngành an toàn thông tin. Môn học này cung cấp các kiến thức căn bản trong việc phát triển và quản lý các biện pháp đảm bảo an toàn thông tin. Môn học cũng giới thiệu các tiêu chuẩn an toàn phổ biến trong nước và quốc tế cũng như các quy định pháp luật về an toàn thông tin mà các giải pháp an toàn được khuyến nghị tuân theo và cần được tuân thủ. Ngoài ra, môn học cũng giới thiệu nguyên tắc và biện pháp giúp cho việc vận hành hệ thống đảm bảo an toàn cũng như duy trì việc hoạt động liên tục và xây dựng kế hoạch ứng phó khi có sự cố.

Bài giảng gồm 7 chương với nội dung như sau.

Chương 1 giới thiệu các mục tiêu và vấn đề cơ bản của quản lý an toàn thông tin. Với sự quan tâm ngày càng tăng về vấn đề an toàn, việc xây dựng các yêu cầu cũng như cách thức đảm bảo an toàn cho các nhiệm vụ, công việc của cơ quan/tổ chức chịu nhiều thách thức. Các yêu cầu và biện pháp an toàn không những phải tuân thủ các ràng buộc về mặt luật pháp mà cả về khía cạnh xã hội thể hiện sự đóng góp của cơ quan/tổ chức tới an toàn chung của cộng đồng.

Chương 2 giới thiệu các khái niệm về việc xây dựng và triển khai các kế hoạch đảm bảo an toàn  thông tin cho hệ thống. Các mục tiêu và tổ chức quản lý an toàn thông tin hiệu quả được trình bày trong phần này. Ngoài ra các vấn đề an toàn cơ bản trong việc xây dựng mô hình đe dọa với ứng dụng cũng được trình bày trong chương này.

Chương 3 tập trung trình bày cách thức phân tích và đánh giá rủi ro của các biện pháp kiểm soát với các vấn đề về an toàn hay các lỗ hổng giúp cho người quản lý có thể ra quyết định phù hợp cũng như xác định mức độ rủi ro chấp nhận được. Cách thức triển khai và đặc trưng của các tiêu chuẩn thực tế cho việc phân tích rủi ro bao gồm OCTAVE, NIST SP 800-30 và ISO 27005 được giới thiệu chi tiết trong phần này.

Chương 4 trình bày về các tiêu chuẩn về an toàn thông tin phổ biến trên thế giới do Tổ chức tiêu chuẩn quốc tế ISO, Viện Tiêu chuẩn và Công nghệ Quốc gia Mỹ NIST ban hành. Chương này chủ yếu giới thiệu bộ tiêu chuẩn IS0 27000 và hệ thống tiêu chuẩn NIST. Phần cuối chương giới thiệu các tiêu chuẩn về an toàn thông tin của Việt Nam đã được công bố.

Chương 5 nêu các yêu cầu căn bản đối với việc vận hành và sử dụng hệ thống cũng như các nhiệm vụ đảm bảo an toàn cần thực hiện. Vấn đề về quy trình quản lý thay đổi trong cấu hình hệ thống và các cách thức kiểm soát thiết bị và dữ liệu cũng được trình bày trong chương này. Bên cạnh đó chương này trình bày các vấn đề cơ bản với việc quản lý  sự cố trong quá trình sử dụng và khai thác hệ thống.

Chương 6 trình bày các vấn đề xây dựng kế hoạch đối phó với những tình huống sự cố để khôi phục hệ thống cũng như đảm bảo khả năng hoạt động của hệ thống trong tình huống tài nguyên hạn chế.

Chương 7 là chương cuối của bài giảng tập trung vào các yêu cầu cơ bản về các chính sách an toàn thông tin của cơ quan hay tổ chức. Các chính sách an toàn này một mặt thể hiện mục tiêu mà cơ quan hay tổ chức đó cần đạt được, mặt khác chúng chứng tỏ sự tuân thủ với các quy định pháp luật cũng như sự đóng góp với xã hội và đối tác về việc đảm bảo an toàn thông tin. Phần tiếp theo của chương giới thiệu các ràng buộc về mặt pháp lý cũng như các hoạt động trong lĩnh vực thông tin và liên lạc của cá nhân và tổ chức cần phải tuân thủ trên lãnh thổ Việt Nam. Phần còn lại của chương giới thiệu các luật quan trọng liên quan đến vấn đề bảo vệ thông tin trong môi trường mạng của các nước Châu Âu, Mỹ và một số quốc gia trong khu vực.

Trong quá trình biên soạn bài giảng, dù tác giả có nhiều cố gắng song không thể tránh được những thiếu sót. Tác giả rất mong muốn nhận được các ý kiến phản hồi và góp ý cho các thiếu sót cũng như cập nhật và hoàn thiện nội dung của bài giảng.

Người biên soạn.

# Mục lục

# Danh mục các hình vẽ

# Danh mục các bảng

# DANH MỤC CÁC THUẬT NGỮ TIẾNG ANH VÀ VIẾT TẮT

| Từ viết tắt | Thuật ngữ tiếng Anh/Giải thích | Thuật ngữ tiếng Việt/Giải thích |
|---|---|---|
| ACL | Access Control List | Danh sách kiểm soát truy nhập |
| CIA | Confidentiality-Integrity-Availability | Bí mật, Toàn vẹn và Sẵn dùng |
| CII | Critical Information Infrastructure | Hạ tầng thông tin quan trọng |
| CSA | Cyber Security Agency | Cơ quan an ninh mạng |
| SOC | Security Operations Centre | Trung tâm giám sát hoạt động an ninh |
| CPU | Central Processing Unit | Đơn vị xử lý trung tâm |
| DAC | Discretionary Access Control | Kiểm soát truy nhập tùy chọn |
| DEP | Data Execution Prevention | Ngăn chặn thực thi dữ liệu |
| EAL | Evaluation Assurance Levels | Mức độ đánh giá an toàn |
| GUI | Graphic User Interface | Giao diện người dùng đồ họa |
| IDE | Integrated Development Environment | Môi trường phát triển tích hợp |
| IDS | Intrusion Detection System | Hệ thống phát hiện xâm nhập |
| ISO | International Standard Organisation | Tổ chức tiêu chuẩn quốc tế |
| ITU | International Telecommunication Union | Liên minh viễn thông quốc tế |
| LSM | Linux Security Module | Mô-đun an ninh Linux |
| ISP | Internet Service Provider | Nhà cung cấp dịch vụ Internet |
| MAC | Mandatory Access Control | Kiểm soát truy nhập bắt buộc |
| PC | Personal Computer | máy tính cá nhân |
| RBAC | Role Based Access Control | Kiểm soát truy nhập theo vai trò |
| TPM | Trusted Platform Module | Mô-đun hạ tầng tin cậy |
| WTO | World Trade Organization | Tổ chức thương mại thế giới |

# CHƯƠNG 1. TỔNG QUAN VỀ QUẢN LÝ AN TOÀN THÔNG TIN

Chương này giới thiệu các mục tiêu và vấn đề cơ bản của quản lý an toàn thông tin. Với sự quan tâm ngày càng tăng về vấn đề an toàn, việc xây dựng các yêu cầu cũng như cách thức đảm bảo an toàn cho các nhiệm vụ, công việc của cơ quan/tổ chức chịu nhiều thách thức. Các yêu cầu và biện pháp an toàn không những phải tuân thủ các ràng buộc về mặt luật pháp mà cả về khía cạnh xã hội thể hiện sự đóng góp của cơ quan/tổ chức tới an toàn chung của cộng đồng.

## 1.1 Vấn đề an toàn thông tin

### 1.1.1 *Giới thiệu*

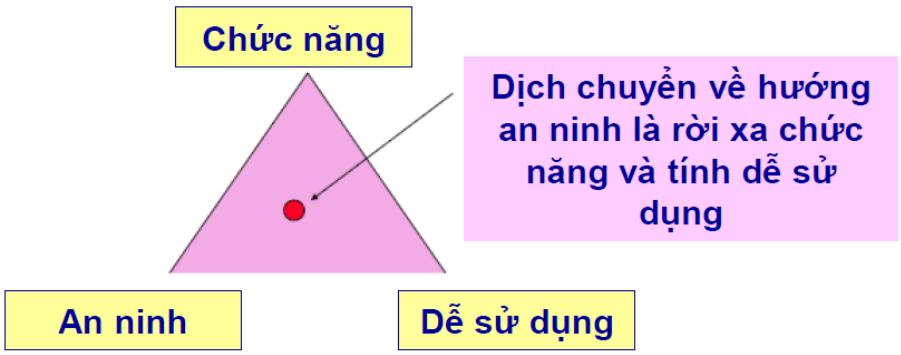
Trên thực tế các cơ quan hay tổ chức có rất nhiều vấn đề quan trọng cần quan tâm và giải quyết với các nhiệm vụ và công việc thường xuyên hơn là việc thực hiện an toàn thông tin. Chẳng hạn như:

- Công ty kinh doanh cần quảng bá và bán sản phẩm để tồn tại và phát triển
- Các cơ quan nhà nước đảm bảo xử lý các yêu cầu của công dân đúng luật và đúng hạn

Với sự phát triển của công nghệ, các cơ quan/tổ chức phải đối mặt với các vấn đề tiêu biểu:

- Mất trộm thông tin về bí mật kinh doanh, khách hàng, lừa đảo
- Các máy tính bị cài đặt phần mềm độc hại để tấn công cơ quan/tổ chức khác
- Các máy tính bị gián đoạn hay tê liệt không thể cung cấp dịch vụ đáp ứng nhu cầu của công ty cũng như khách hàng.

Các hoạt động bảo vệ thông tin và các thành phần thiết yếu bao gồm hệ thống và phần cứng mà sử dụng, lưu trữ, chuyển tiếp thông tin đó cho tới việc áp dụng các chính sách, các chương trình đào tạo và công nghệ có vai trò tối quan trọng để các công việc của cơ quan/tổ chức được diễn ra một cách bình thường. Đây là quá trình tiếp diễn và liên tục do những giới hạn về nguồn nhân lực và tài chính. Như vậy, cần cân bằng giữa nhu cầu đảm bảo an toàn cho các tài nguyên thông tin và việc thực hiện các hoạt động bình thường của cơ quan/tổ chức như thể hiện trong hình dưới đây.




**Hình 1-1. Tương quan giữa các yêu cầu hệ thống**

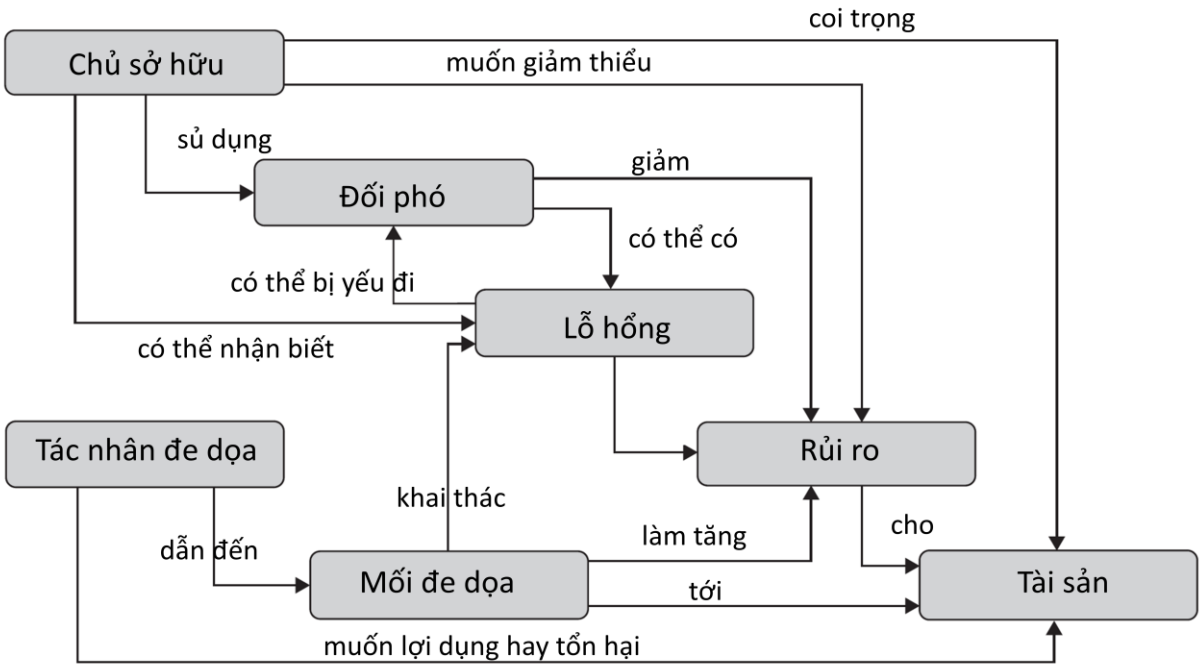
Các biện pháp bảo đảm an toàn cho hệ thống và hỗ trợ các chức năng của hệ thống để công việc được thực hiện một cách đầy đủ chứ không phải chỉ là các biện pháp hạn chế hay ràng buộc việc truy cập đến các phương tiện hay tài nguyên cần thiết. Đồng thời, các biện pháp kiểm soát cũng cần thuận tiện và dễ hiểu với người dùng để tránh việc việc chối bỏ hay thiếu sót khi thực hiện.

### 1.1.2 *Các chủ thể an toàn*

Để xác định một cách đúng đắn các vấn đề về an toàn cũng như sự ảnh hưởng của chúng lên những thông tin cần được bảo vệ, người ta thường sử dụng sơ đồ phân tích đánh giá liên quan giữa các chủ thể an toàn thông tin.

Hình 1-2 mô tả mối tương quan giữa ba đối tượng quan trọng trong phân tích và đánh giá an toàn là tài sản, chủ sở hữu tài sản và các tác nhân tác động lên tài sản đó. Việc nhận thức thích đáng quan hệ giữa các đối tượng này cho phép hiểu được giá trị của tài sản cần bảo vệ, mức độ rủi ro của mối đe dọa cũng như tính hiệu quả của các biện pháp đối phó. Các khái niệm cơ bản mô tả trong hình gồm có:

- *Tài sản* (*Asset*) là những thứ (có giá trị) thuộc sở hữu của cơ quan/tổ chức muốn được bảo vệ. Tài sản có thể là thứ cụ thể như cơ sở dữ liệu hoặc trừu tượng như tên tuổi (danh tiếng).
- *Tấn công* (*Attack*) là hành động lợi dụng lỗ hổng để xâm hại, ăn trộm, tung ra, làm hỏng hay phát tán, hay sửa đổi trái phép một tài sản.
- *Biện pháp đối phó* (*Counter-measure*) là các phương pháp nhằm giảm bớt hậu quả của các lỗ hổng. Biện pháp đối phó có thể thuần túy lô-gíc như áp dụng chính sách hay có thể là phần cứng như tường lửa.
- *Rủi ro* (*Risk*) được coi như khả năng sự kiện không mong muốn xảy ra thường ám chỉ đến các tổn thất có thể và thường được đối phó bằng việc triển khai: các công cụ kiểm tra giám sát; chuyển cho bên thứ ba như bảo hiểm; giảm nhẹ tổn thất do mất mát bằng lập kế hoạch đối phó với bất ngờ. Rủi ro thặng dư là rủi ro còn lại sau khi mọi biện pháp thận trọng đã được thực thi. Rủi ro chấp nhận được là rủi ro mà cơ quan/tổ chức chấp nhận sau khi đã hoàn tất chương trình quản lý rủi ro.




**Hình 1-2. Quan hệ giữa các chủ thể an toàn thông tin**

- *Đe dọa* (*Threat*) hướng tới việc phân loại các vấn đề có thể xảy ra cho tài sản của cơ quan/tổ chức. Đe dọa là các hành động chưa xảy ra nhưng khả năng xảy ra của chúng có thể thấy được.
- *Tác nhân đe dọa* (*Threat agent*) là các chủ thể cụ thể của các mối đe dọa không giới hạn ở con người.
- *Lỗ hổng* (*Vulnerability*) là cơ hội dẫn đến việc các mối đe dọa trở thành hiện thực và ảnh hưởng đến các tài sản. Lỗ hổng không chỉ giới hạn ở phần cứng, phần mềm mà có thể lỗi do quy trình.

Các mối đe dọa có thể được phân thành các loại như sau:

- Các hành động do lỗi của con người hay lỗi:
  - Các đe dọa này bao gồm các hoạt động được thực hiện vô tình bởi người dùng được phép.
  - Thiếu kinh nghiệm, đào tạo không đầy đủ, nhầm lẫn cũng như không tuân thủ quy trình, chính sách và quy định có thể biến nhân viên tốt thành tác nhân gây hại. Điều này dẫn đến việc đe dọa tính bí mật, toàn vẹn và sẵn sàng của dữ liệu
- Xâm phạm sở hữu trí tuệ. Sở hữu trí tuệ có thể gồm các bí mật thương mại, bản quyền, nhãn hiệu và bằng phát minh. Việc chiếm đoạt trái phép dẫn đến việc đe dọa an toàn thông tin.
- Các hành động xâm phạm và gián điệp:
  - Hoạt động của con người hay điện tử có thể dẫn đến lộ bí mật thông tin.

- Các tác nhân đe dọa có thể dùng nhiều phương pháp khác nhau để truy nhập tài sản thông tin. Có một số cách hợp pháp như sử dụng trình duyệt Web để thu thập thông tin. Song, gián điệp công nghệ là cách phi pháp. Tuy nhiên có thể sử dụng hành động thông thường như xem trộm hay hoạt động sử dụng công nghệ cao.

- Hành động làm biến đổi thông tin xảy ra khi kẻ tấn công hay nhân viên nội bộ đánh cắp thông tin và yêu cầu bồi thường để trả lại hay chấp thuận không công bố thông tin đó.
- Hành động phá hoại/ngầm liên quan đến việc phá hoại ngầm hệ thống máy tính hay công việc kinh doanh hay phá hoại hoặc phá hủy tài sản hay hình ảnh của cơ quan/tổ chức. Các hành động này có thể thay đổi từ hành động phá hoại lặt vặt của nhân viên cho đến phá hoại có chủ đích, từ kẻ bẻ khóa cho đến khủng bố mạng.
- Hành động của kẻ trộm là việc lấy đi trái phép tài sản của người khác. Tài sản có thể là đối tượng cụ thể hoặc điện tử hay trí tuệ. Giá trị tài sản bị mất đi khi nó bị sao chép hay lấy đi mà chủ sở hữu không biết.
- Các mối đe dọa phần mềm là những thứ liên quan đến chương trình máy tính được phát triển nhằm mục đích làm hỏng, phá hủy hay từ chối phục vụ cho hệ thống của cơ quan/tổ chức. Có thể kể một số dạng phần mềm có mục đích xấu như: vi-rút máy tính, sâu, hay phần mềm gián điệp (trojan horse).
- Thiên tai là mối đe dọa nguy hiểm nhất do chúng xảy ra mà ít có cảnh báo và nằm ngoài tầm kiểm soát của con người như hỏa hoạn, lũ lụt, động đất, sấm sét.
- Sai lệch các dịch vụ làm gián đoạn hệ thống thông tin do hệ thống cần sự hoạt động thành công của nhiều hệ thống hỗ trợ như mạng điện, hệ thống viễn thông, và thậm chí các nhân viên gác cổng. Các đe dọa dẫn đến sai lệch chất lượng dịch vụ thể hiện rõ ràng trong vụ tấn công. Việc này dẫn đến gián đoạn tính sẵn sàng
- Hư hỏng phần cứng là các lỗi khi nhà sản xuất phân phối các thiết bị. Các lỗi này làm hệ thống hoạt động không như mong muốn dẫn đến dịch vụ không tin cậy hay thiếu tính sẵn sàng.
- Hư hỏng phần mềm là mối đe dọa thường xuyên do số lượng lớn các mã máy tính được viết, cung cấp và bán trước khi các lỗi được phát hiện và giải quyết. Đôi khi việc kết hợp phần cứng và phần mềm nhất định lại gây lỗi.
- Lỗi thời về công nghệ có thể xảy ra khi hạ tầng cũ hay lỗi thời dẫn đến hệ thống không ổn định và không tin cậy. Điều này dẫn đến rủi ro mất tính toàn vẹn dữ liệu do các cuộc tấn công tiềm tàng.

## 1.2 Mục tiêu an toàn thông tin

### 1.2.1 *Tính sẵn dùng, toàn vẹn, và bí mật*

Các mục tiêu cốt lõi của an toàn thông tin là để đảm bảo tính sẵn dùng, tính toàn vẹn và bí mật cho các tài sản quan trọng. Mỗi tài sản sẽ yêu cầu các mức bảo vệ khác nhau. Tất cả các biện pháp kiểm soát, cơ chế và biện pháp bảo vệ an ninh được thực hiện để cung cấp một hoặc nhiều mức bảo vệ này. Ngoài ra các rủi ro, mối đe dọa và lỗ hổng cần được đánh giá về khả năng phá vỡ một hoặc tất cả các nguyên tắc sẵn dùng, toàn vẹn và bí mật.

Bảo vệ tính sẵn sàng đảm bảo độ tin cậy và truy cập kịp thời vào dữ liệu và tài nguyên cho các cá nhân được ủy quyền. Thiết bị mạng, máy tính và ứng dụng phải cung cấp chức năng phù hợp để thực hiện theo cách có thể dự đoán được với mức hiệu suất có thể chấp nhận được. Các thiết bị và ứng dụng này sẽ có thể phục hồi từ trường hợp lỗi hay gián đoạn theo cách an toàn và nhanh chóng để năng suất không bị ảnh hưởng một cách tiêu cực. Cần có các cơ chế bảo vệ cần thiết để chống lại các mối đe dọa bên trong và bên ngoài có thể ảnh hưởng đến tính sẵn dùng và năng suất của tất cả các thành phần xử lý công việc. Việc đảm bảo sự sẵn có của các nguồn lực cần thiết trong cơ quan/tổ chức có vẻ dễ thực hiện hơn thực tế. Mạng có rất nhiều phần mà phải hoạt động (bộ định tuyến, máy chủ DNS, máy chủ DHCP, proxy, tường lửa…). Cũng như vậy, phần mềm có nhiều thành phần phải được thực hiện một cách lành mạnh (hệ điều hành, ứng dụng, phần mềm chống phần mềm độc hại). Có những vấn đề môi trường có thể ảnh hưởng tiêu cực đến hoạt động của cơ quan/tổ chức (hỏa hoạn, lũ lụt, các vấn đề về điện), thiên tai tiềm năng và hành vi trộm cắp hay tấn công vật lý. Cơ quan/tổ chức phải hiểu đầy đủ về môi trường hoạt động và các điểm yếu sẵn có của nó để có thể đưa ra các biện pháp đối phó thích hợp.

Tính toàn vẹn được duy trì khi đảm bảo tính chính xác và độ tin cậy của thông tin mà hệ thống cung cấp và bất kỳ sửa đổi trái phép nào đều được ngăn chặn. Các cơ chế phần cứng, phần mềm và truyền thông phải làm việc một cách hài hòa để duy trì và xử lý dữ liệu một cách chính xác và di chuyển dữ liệu đến các đích dự định mà không bị thay đổi bất thường. Các hệ thống và mạng phải được bảo vệ chống lại sự can thiệp và hư hỏng bên ngoài. Các môi trường đảm bảo thuộc tính an toàn này cần chắc chắn rằng những kẻ tấn công hoặc những sai lầm của người dùng không làm tổn hại đến tính toàn vẹn của các hệ thống hoặc dữ liệu. Khi kẻ tấn công chèn virus, bom logic hoặc cửa sau vào hệ thống dẫn đến tính toàn vẹn của hệ thống bị xâm phạm. Thông tin được lưu trữ trên hệ thống bị làm hỏng, sửa đổi một cách độc hại hoặc thay thế dữ liệu bằng dữ liệu không chính xác. Việc kiểm soát truy cập chặt chẽ, phát hiện xâm nhập và kỹ thuật băm có thể chống lại các mối đe dọa này.

Người dùng thông thường tác động đến toàn bộ hệ thống hoặc tính toàn vẹn của dữ liệu (mặc dù người dùng nội bộ cũng có thể phạm các hành động độc hại). Ví dụ, người dùng có truy nhập tới toàn bộ ổ đĩa cứng có thể vô tình xóa các file cấu hình vì cho rằng

rằng việc xóa file không sao. Hoặc người dùng có thể chèn các giá trị không chính xác vào ứng dụng xử lý dữ liệu tính phí khách hàng 3 triệu thay vì 3 trăm nghìn. Việc sửa đổi dữ liệu không chính xác được lưu giữ trong cơ sở dữ liệu là cách phổ biến mà người dùng có thể vô tình làm hỏng dữ liệu và có thể có tác động lâu dài.

Bí mật đảm bảo rằng mức độ che dấu cần thiết được thực thi tại mỗi giao tiếp xử lý dữ liệu và ngăn chặn việc tiết lộ trái phép. Các biện pháp bảo mật này được sử dụng phổ biến khi dữ liệu nằm trên các hệ thống và thiết bị trong mạng, ngay khi nó được truyền đi và khi đến đích. Những kẻ tấn công có thể ngăn chặn các cơ chế bảo mật bằng cách theo dõi mạng, nhìn trộm, ăn cắp các file mật khẩu, bẻ khóa các chương trình mã hóa và kỹ thuật xã hội.

Kỹ thuật xã hội là khi một người lừa một người khác để chia sẻ thông tin bí mật, ví dụ, bằng cách giả làm người được ủy quyền để có quyền truy cập vào thông tin đó. Kỹ thuật xã hội có thể có nhiều hình thức. Bất kỳ phương tiện truyền thông một-một có thể được sử dụng để thực hiện các cuộc tấn công sử dụng kỹ thuật xã hội. Người dùng có thể cố ý hoặc vô tình tiết lộ thông tin nhạy cảm bằng cách không mã hóa thông tin nhạy cảm trước khi gửi cho người khác, chia sẻ bí mật thương mại của công ty hoặc không sử dụng cẩn thận để bảo vệ thông tin bí mật khi xử lý thông tin đó.

Bảo mật có thể được đảm bảo bằng cách mã hóa dữ liệu khi nó được lưu trữ và truyền đi, thực thi kiểm soát truy cập chặt chẽ và phân loại dữ liệu, và bằng cách đào tạo nhân viên về các thủ tục bảo vệ dữ liệu thích hợp. Tính sẵn dùng, tính toàn vẹn và bảo mật là các nguyên tắc bảo mật quan trọng. Cần hiểu ý nghĩa của các biện pháp này và cách chúng được cung cấp bởi các cơ chế khác nhau, và sự thiếu vắng của chúng có thể ảnh hưởng tiêu cực đến cơ quan/tổ chức.

Trong thực tế, khi xử lý vấn đề an toàn thông tin nó thường chỉ được xem xét thông qua lăng kính của bí mật. Các mối đe dọa về tính toàn vẹn và tính sẵn dùng có thể bị bỏ qua và chỉ được xử lý sau khi chúng bị xâm phạm. Một số tài sản có yêu cầu quan trọng về bảo mật (bí mật thương mại của công ty), một số khác có yêu cầu quan trọng về tính toàn vẹn (giá trị giao dịch tài chính) và một số khác yêu cầu về tính sẵn sàng (máy chủ web thương mại điện tử). Nhiều người hiểu các khái niệm về bộ ba yêu cầu này nhưng có thể không hoàn toàn lường trước sự phức tạp của việc thực hiện các biện pháp kiểm soát cần thiết để cung cấp tất cả các mức độ bảo vệ cần thiết.

### 1.2.2 *Các thuộc tính khác*

Ngoài bộ ba bí mật, sẵn sàng, và toàn vẹn, cần xem xét rất nhiều khái niệm và nguyên tắc liên quan đến bảo mật khác khi thiết kế chính sách bảo mật và triển khai giải pháp bảo mật liên quan đến xác thực, ủy quyền và kiểm toán. Các vấn đề này thực sự đề cập đến năm yếu tố: định danh, xác thực, cấp quyền, kiểm toán và kế toán.

- Định danh: Tuyên bố là một danh tính khi cố gắng truy cập vào một khu vực hoặc hệ thống được bảo vệ

- Xác thực: Chứng minh rằng danh tính là hợp lệ
- Cấp quyền: Xác định quyền (tức là cho phép và/hoặc từ chối) quyền truy cập tài nguyên và đối tượng cho một danh tính cụ thể
- Kiểm toán: Ghi lại nhật ký các sự kiện và hoạt động liên quan đến hệ thống và các đối tượng
- Kế toán (hay còn gọi là trách nhiệm giải trình): Xem xét các file log để kiểm tra sự tuân thủ và các vi phạm nhằm yêu cầu các đối tượng chịu trách nhiệm về hành động của mình.

Các yếu tố này thực sự là một khái niệm nền tảng cho bảo mật. Thiếu bất kỳ yếu tố nào trong số năm yếu tố này có thể dẫn đến cơ chế bảo mật không hoàn chỉnh.

Chính sách bảo mật của tổ chức chỉ có thể được thực thi đúng cách nếu duy trì được trách nhiệm giải trình. Nói cách khác, chỉ có thể duy trì bảo mật nếu các đối tượng phải chịu trách nhiệm về hành động của họ. Trách nhiệm giải trình hiệu quả dựa vào khả năng chứng minh danh tính của chủ thể và theo dõi các hoạt động của họ. Trách nhiệm giải trình được thiết lập bằng cách liên kết con người với các hoạt động của danh tính trực tuyến thông qua các dịch vụ bảo mật và cơ chế kiểm tra, ủy quyền, xác thực và định danh. Do đó, trách nhiệm giải trình của con người cuối cùng phụ thuộc vào sức mạnh của quá trình xác thực. Nếu không có quy trình xác thực chắc chắn, không thể tin chắn rằng con người được liên kết với một tài khoản cụ thể là thực thể thực sự kiểm soát tài khoản người dùng đó khi hành động không mong muốn xảy ra.

Để có trách nhiệm giải trình khả thi, có thể cần có khả năng hỗ trợ các quyết định bảo mật và việc thực hiện chúng trước pháp luật. Nếu không thể hỗ trợ hợp pháp các nỗ lực bảo mật của mình, thì sẽ khó có thể quy trách nhiệm cho người dungf về các hành động được gắn với tài khoản người dùng. Chỉ với một mật khẩu làm xác thực, có rất nhiều lỗ hổng. Mật khẩu là hình thức xác thực kém an toàn nhất, với hàng chục phương pháp có thể để xâm phạm chúng. Tuy nhiên, với việc sử dụng kết hợp xác thực đa yếu tố, chẳng hạn như mật khẩu, thẻ thông minh và quét vân tay, có rất ít khả năng bất kỳ người nào khác có thể xâm phạm quá trình xác thực để mạo danh người chịu trách nhiệm về tài khoản người dùng.

Quan điểm của bảo mật là giữ cho những điều xấu không xảy ra trong khi duy trì và đảm bảo những điều tốt đẹp. Khi điều tồi tệ xảy ra, các cơ quan/tổ chức thường mong muốn sự hỗ trợ từ cơ quan thực thi pháp luật và hệ thống pháp luật để được bảo vệ hoặc bồi thường. Như vậy, cơ quan/tổ chức phải chứng minh rằng tội phạm đã được thực hiện, nghi phạm đã phạm tội đó và cơ quan/tổ chức đã nỗ lực hợp lý để ngăn chặn tội phạm. Cuối cùng, điều này đòi hỏi một giải pháp bảo mật hoàn chỉnh có kỹ thuật xác thực đa yếu tố mạnh mẽ, cơ chế ủy quyền vững chắc và hệ thống kiểm tra hoàn hảo. Ngoài ra, cơ quan/tổ chức phải chứng minh rằng sự tuân thủ tất cả các luật và quy định hiện hành, rằng các cảnh báo và thông báo thích hợp đã được đăng, rằng cả bảo mật logic và vật lý đều không bị xâm phạm và không có cách giải thích hợp lý nào khác về bằng chứng điện tử. Đây là một tiêu chuẩn khá khó để đáp ứng. Do đó, cơ quan/tổ chức nên đánh giá cơ

sở hạ tầng bảo mật của mình và nỗ lực để thiết kế và thực hiện bảo mật có thể bảo vệ được về mặt pháp lý.

### 1.2.3 *Các cơ chế bảo vệ*

Cơ chế bảo vệ là đặc trưng chung của các biện pháp kiểm soát an toàn. Không phải tất cả các biện pháp kiểm soát bảo mật đều phải có tất cả các thuộc tính an toàn, nhưng nhiều biện pháp kiểm soát cung cấp khả năng bảo vệ tính bảo mật, tính toàn vẹn và tính sẵn dụng thông qua việc sử dụng các cơ chế này. Ví dụ phổ biến về các cơ chế này bao gồm *phân lớp* hoặc cấp độ truy cập, *sử dụng tính trừu tượng, ẩn dữ liệu* và sử dụng *mã hóa*.

Phân lớp, còn được gọi là phòng thủ theo chiều sâu, chỉ đơn giản là việc sử dụng nhiều điều khiển theo chuỗi. Không biện pháp kiểm soát riêng lẻ có thể bảo vệ chống lại tất cả các mối đe dọa có thể xảy ra. Sử dụng giải pháp nhiều lớp cho phép nhiều biện pháp kiểm soát khác nhau để bảo vệ chống lại bất kỳ mối đe dọa nào xảy ra. Khi các giải pháp bảo mật được thiết kế theo từng lớp, việc kiểm soát không thành công sẽ không dẫn đến việc hệ thống hoặc dữ liệu bị lộ.

Sử dụng các lớp theo chuỗi thay vì song song là quan trọng. Thực hiện các hạn chế an toàn theo chuỗi có nghĩa là thực hiện lần lượt theo kiểu tuyến tính. Chỉ thông qua một cấu hình chuỗi, mỗi cuộc tấn công sẽ được quét, đánh giá hoặc giảm thiểu bởi mọi biện pháp kiểm soát an ninh. Trong cấu hình chuỗi, lỗi của một kiểm soát bảo mật không làm cho toàn bộ giải pháp không hiệu quả. Nếu các biện pháp kiểm soát bảo mật được triển khai song song, một mối đe dọa có thể thoát qua trạm kiểm soát duy nhất không phát hiện hoạt động độc hại cụ thể của nó.

Phân lớp cũng cho phép mạng bao gồm nhiều thực thể riêng biệt, mỗi thực thể có các kiểm soát bảo mật và lỗ hổng bảo mật riêng biệt. Trong giải pháp bảo mật hiệu quả, việc hợp lực giữa tất cả các hệ thống được nối mạng để tạo ra hàng rào bảo mật duy nhất. Việc sử dụng các hệ thống bảo mật tách biệt tạo ra giải pháp bảo mật nhiều lớp.

*Trừu tượng hóa* được sử dụng cho tính hiệu quả. Các phần tử tương tự được đưa vào nhóm, lớp hoặc vai trò được gán cho biện pháp bảo mật, hạn chế hoặc quyền như một nhóm. Như vậy, việc trừu tượng hóa được sử dụng khi phân loại các đối tượng hoặc gán vai trò cho các chủ thể. Việc trừu tượng hóa cũng bao gồm định nghĩa của các loại đối tượng và chủ thể hoặc của chính các đối tượng (nghĩa là, một cấu trúc dữ liệu được sử dụng để xác định một khuôn mẫu cho một lớp thực thể). Tính trừu tượng được sử dụng để xác định những loại dữ liệu mà một đối tượng có thể chứa, những loại chức năng nào có thể được thực hiện trên hoặc bởi đối tượng đó và những khả năng mà đối tượng đó có. Tính trừu tượng đơn giản hóa bảo mật bằng cách cho phép gán các kiểm soát an toàn cho một nhóm đối tượng được thu thập theo loại hoặc chức năng.

*Ẩn dữ liệu* chính xác là việc ngăn đối tượng phát hiện hoặc truy cập dữ liệu bằng cách định vị dữ liệu trong kho chứa mà đối tượng không thể truy cập hoặc nhìn thấy. Các

hình thức ẩn dữ liệu bao gồm giữ cho cơ sở dữ liệu không bị truy cập bởi những người truy cập trái phép và hạn chế đối tượng ở cấp thấp hơn truy cập dữ liệu ở cấp cao hơn. Việc ngăn chặn ứng dụng truy cập trực tiếp vào phần cứng cũng là một hình thức ẩn dữ liệu. Ẩn dữ liệu thường là một yếu tố quan trọng trong kiểm soát bảo mật cũng như trong lập trình.

Thuật ngữ bảo mật thông qua việc giấu diếm có thể hợp. Tuy nhiên ẩn dữ liệu là hành động cố ý định vị dữ liệu để đối tượng trái phép không thể xem hoặc truy cập được, trong khi bảo mật thông qua giấu diếm là ý tưởng không thông báo cho đối tượng về một đối tượng đang hiện diện và do đó hy vọng rằng đối tượng sẽ không phát hiện ra đối tượng. Bảo mật thông qua giấu diếm thực tế không thực hiện bất kỳ hình thức bảo vệ nào. Thay vào đó, đó là một nỗ lực để hy vọng một điều gì đó quan trọng không bị phát hiện bằng cách giữ bí mật về kiến thức về nó. Tương tự như khi một lập trình viên nhận thức được lỗ hổng trong mã phần mềm, nhưng lại lờ đi với hy vọng không ai phát hiện ra vấn đề và khai thác nó.

*Mã hóa* là khoa học che giấu ý nghĩa hoặc mục đích của thông tin trao đổi khỏi những người nhận không chủ ý. Mã hóa có thể có nhiều dạng và được áp dụng cho mọi loại liên lạc điện tử, bao gồm các file văn bản, âm thanh và video cũng như bản thân các ứng dụng. Mã hóa là một yếu tố quan trọng trong biện pháp an toàn, đặc biệt là liên quan đến việc truyền dữ liệu giữa các hệ thống. Có nhiều điểm mạnh khác nhau của mã hóa, mỗi điểm mạnh được thiết kế thích hợp cho một mục đích sử dụng cụ thể. Mã hóa yếu không có gì khác hơn là sự xáo trộn thông tin đơn giản hoặc thậm chí có khả năng bảo mật thông qua sự giấu diếm.

## 1.3 Hệ thống khung an toàn thông tin

### 1.3.1 *Chương trình an toàn*

Đảm bảo an toàn thông tin cho cơ quan/tổ chức luôn là vấn đề quan trọng ngay tại thời điểm khởi đầu cũng như trong suốt quá trình hoạt động và phát triển của cơ quan/tổ chức đó. Sự phát triển của công nghệ, máy tính và phương tiện mạng cũng như cách thức hoạt động của cơ quan/tổ chức khiến cho vấn đề an toàn trở nên rất phức tạp từ việc đảm bảo an toàn cho các phần mềm, máy tính cho đến các vấn đề về việc quản lý hệ thống mạng.

Chương trình an toàn (*security program*) của cơ quan/tổ chức không được xây dựng từ chân không mà là một hệ thống (*framework*) gồm nhiều thực thể: các cơ chế bảo vệ vật lý, quản trị và lô-gíc; các thủ tục; quy trình làm việc; con người. Toàn bộ các thành phần này phối hợp với nhau để tạo nên các lớp bảo vệ cho môi trường hoạt động an toàn. Bởi vì chương trình an toàn là một khung, các cơ quan/tổ chức được tự do gắn các loại công nghệ, phương pháp và thủ tục khác nhau để đạt được mức độ bảo vệ cần thiết cho môi trường của họ.

Các tiêu chuẩn về an toàn thông tin giúp xây dựng các chương trình an toàn một cách thích đáng và phù hợp với hoàn cảnh của cơ quan/tổ chức cụ thể. Một cách tiếp cận để xây dựng chương trình an toàn là sửa đổi hay làm theo mô hình hoặc khung an toàn thông tin tiêu chuẩn. Trong đó, khung là cấu trúc xương sống mà trong đó việc lập kế hoạch thiết kế chi tiết có thể được dùng khi phát triển chương trình cụ thể. Kinh nghiệm cho thấy rằng không có thiết kế nào hoàn hảo cho mọi cơ quan tổ chức.

Tiêu chuẩn ISO 17799 và bộ tiêu chuẩn 27000 thường được tham khảo để hướng dẫn cách thức xây dựng và duy trì hệ thống quản lý an toàn thông tin ISMS (*Information Security Management System*) hay còn được gọi là chương trình an toàn. Mục tiêu để cung cấp các hướng dẫn cho các cơ quan/tổ chức về cách thiết kế, thực hiện và duy trì các chính sách, quy trình và công nghệ để quản lý rủi ro đối với các tài sản thông tin nhạy cảm.

Lý do mà các tiêu chuẩn được sử dụng mà thậm chí còn cần thiết chính là nỗ lực và quản lý tập trung các biện pháp kiểm soát an toàn khác nhau được triển khai trên toàn bộ cơ quan/tổ chức. Nếu không có một hệ thống quản lý an toàn, các biện pháp kiểm soát được thực hiện và quản lý một cách riêng lẻ và rời rạc. Bộ phận CNTT sẽ theo dõi các giải pháp công nghệ còn an toàn nhân sự sẽ nằm trong bộ phận tổ chức hay hành chính, đảm bảo an ninh vật lý do bộ phận quản lý vật tư thiết bị, và duy trì hoạt động do bộ phận vận hành. Bộ tiêu chuẩn như ISO cung cấp phương tiện để giám sát tất cả các vấn đề này và kết hợp chúng lại với nhau một cách toàn diện.

### 1.3.2 *Kiến trúc an toàn doanh nghiệp*

Cơ quan tổ chức mong muốn đảm bảo an toàn cho môi trường làm việc của mình một cách thống nhất có thể lựa chọn:

- Cách 1: chọn một giải pháp có sẵn và sử dụng để phục vụ cho yêu cầu an toàn
- Cách 2: Tìm hiểu môi trường làm việc và các yêu cầu an toàn với công việc và môi trường hoạt động, vạch ra khung chương trình và chiến lược hay có thể kết hợp cả hai.

Khi phát triển một kiến trúc, trước tiên cần xác định các bên liên quan phải có. Đó là ai sẽ theo dõi và sử dụng kiến trúc. Tiếp theo, các góc độ khác nhau cần được phát triển sao cho việc này phản ánh cách các thông tin quan trọng đối với các bên liên quan khác nhau và chúng được biểu diễn một cách hữu ích nhất. Nhân viên điều hành cần nhìn công ty từ quan điểm kinh doanh, người xây dựng quy trình hoạt động cần hiểu loại thông tin nào cần được thu thập để hỗ trợ thực hiện nhiệm vụ hay hoạt động kinh doanh; người phát triển ứng dụng cần hiểu các yêu cầu hệ thống để duy trì và xử lý thông tin; người lập mô hình dữ liệu cần biết cách cấu trúc các phần tử dữ liệu và nhóm công nghệ cần hiểu các thành phần mạng cần thiết để hỗ trợ các lớp ở trên nó. Tất cả các bên đều nhìn vào cùng một kiến trúc của cùng một cơ quan/tổ chức, song nó chỉ được trình bày theo quan điểm mà họ hiểu và có liên quan trực tiếp đến trách nhiệm của họ trong cơ quan/tổ chức.

Việc xây dựng kiến trúc doanh nghiệp không chỉ giúp hiểu cơ quan/tổ chức từ nhiều góc độ khác nhau mà còn hiểu sự tác động của việc thay đổi tới các lớp, thành phần khác nhau của cơ quan/tổ chức.

Kiến trúc an toàn doanh nghiệp là kiến trúc con của kiến trúc doanh nghiệp, xác định chiến lược an toàn thông tin bao gồm giải pháp, quy trình, thủ tục và cách thức chúng liên kết trong doanh nghiệp. Việc xây dựng kiến trúc an toàn là cách tiếp cận toàn diện và chặt chẽ để mô tả cấu trúc và hành vi của tất cả các thành phần tạo nên một hệ thống quản lý an toàn thông tin toàn diện. Mục tiêu kiến trúc an toàn để cân đối giữa các nỗ lực về an ninh với thực tiễn hoạt động của cơ quan/tổ chức bao gồm:

- Động lực hoạt động/kinh doanh và các yêu cầu về quy định pháp luật phải phù hợp và thể hiện trong kiến trúc an toàn.
- Các giải pháp an ninh cần phải làm cho công việc của cơ quan được tốt hơn. Các giải pháp an toàn cần cân bằng giữa việc đảm bảo an ninh cho môi trường làm việc và cho phép các chức năng hoạt động ở cấp độ nhất định để không ảnh hưởng tới năng suất của cơ quan/tổ chức.
- Đảm bảo hiệu quả an ninh cân đối giữa chi phí và hiệu quả thu được.

| | TÀI SẢN (What) | ĐỘNG CƠ (Why) | QUY TRÌNH (How) | CON NGƯỜI (Who) | VỊ TRÍ (Where) | THỜI ĐIỂM (When) |
|---|---|---|---|---|---|---|
| Ngữ cảnh | Công việc | Mô hình rủi ro công việc/kinh doanh | Mô hình quy trình công viêc/kinh doanh | Tổ chức công việc và các quan hệ | Vị trí hoạt động | Phụ thuộc thời điểm hoạt động |
| Khái niệm | Hồ sơ các đặc trưng công việc | Kiểm soát các mục tiêu khách quan | Các chiến lược an toàn và phân lớp kiến trúc | Khung tin cậy và mô hình thực thể an ninh | Mô hình miền an toàn | Các mốc thời gian và chu kỳ liên quan an toàn |
| Lô-gíc | Mô hình thông tin công việc/kinh doanh | Các chính sách an toàn | Các dịch vụ an toàn | Hồ sơ đặc quyền và lược đồ thực thể | Các liên kết và mô tả miền an toàn | Chu trình xử lý an toàn |
| Vật lý | Mô hình dữ liệu công việc/kinh doanh | Thủ tục, thực tiễn, quy đinh an toàn | Cơ chế an toàn | Giao tiếp người dùng, ứng dụng, người dùng | Nền tảng và hạ tầng mạng | Thực thi cấu trúc kiểm soát |
| Bộ phận | Cấu trúc dữ liệu chi tiết | Các tiêu chuẩn an toàn | Công cụ và sản phẩm an toàn | Định danh, chức năng, hành động và ACL | Quy trình, nút, địa chỉ và giao thức | Phân chuỗi và định thời các giai đoạn an toàn |
| Vận hành | Đảm bảo hoạt động liên tục | Quản lý rủi ro vận hành | Quản lý và hỗ trợ dịch vụ an toàn | Quản lý và hỗ trợ người dùng và ứng dụng | An toàn cho vị trí, mạng và hệ thống nền tảng | Lịch hoạt động an toàn |

**Hình 1-3. Khung kiến trúc an toàn SABSA**

SABSA là cấu trúc khung và phương pháp luận cho xây dựng kiến trúc an toàn doanh nghiệp và quản lý dịch vụ. Vì là cấu trúc khung nó cung cấp cấu trúc cho xây dựng các kiến trúc riêng lẻ. Vì đây cũng là một phương pháp nên nó cung cấp các quy trình để xây dựng và duy trì kiến trúc này. SABSA cung cấp mô hình vòng đời để kiến trúc có thể được theo dõi liên tục và cải thiện theo thời gian.

Như trong Hình 1-3, mô hình SABSA được phân lớp với lớp đầu tiên xác định các yêu cầu nghiệp vụ từ quan điểm an toàn. Mỗi lớp của mô hình giảm trừu tượng và tăng chi tiết để xây dựng dựa trên những lớp khác và chuyển từ chính sách sang việc triển khai thực tế về công nghệ và giải pháp. Ý tưởng cơ bản là cung cấp một chuỗi có khả năng truy vết thông qua các cấp độ: chiến lược, khái niệm, thiết kế, triển khai.

## 1.4 Quản lý an toàn thông tin

Các tin tức về vi rút gây thiệt hại hàng triệu đô la, tin tặc từ khắp nơi trên thế giới thu thập thông tin thẻ tín dụng từ các tổ chức tài chính hay các trang web của các tập đoàn lớn và các hệ thống của chính phủ bị tấn công vì lý do chính trị là những khía cạnh hấp dẫn về an toàn thông tin. Thực tế, những hoạt động này không phải là những gì mà công ty hoặc chuyên gia thường phải đối phó khi nói đến các nhiệm vụ an toàn hàng ngày

Quản lý an toàn đã thay đổi vì môi trường mạng, máy tính và các ứng dụng thông tin đã thay đổi. Trước đây, thông tin được sử dụng chủ yếu trong các máy chủ, hoạt động trong các mạng tập trung. Chỉ có một số người được phép truy cập và chỉ một nhóm nhỏ người biết cách làm việc của máy chủ. Những điều này làm giảm đáng kể rủi ro an ninh. Ngày nay, hầu hết các mạng tràn ngập các máy tính cá nhân hay thiết bị di động có phần mềm tiên tiến và khả năng xử lý mạnh; người dùng hiểu biết đủ về các hệ thống để có thể gây nguy hiểm; và thông tin không được tập trung trong một máy chủ. Thay vào đó, thông tin "sống" trên máy chủ, máy trạm, máy tính xách tay, thiết bị không dây, thiết bị di động, cơ sở dữ liệu và các mạng khác. Thông tin đi qua các kết nối hữu tuyến và vô tuyến với tốc độ khó hình dung được so với thời gian trước đây.

Mạng Internet và mạng nội bộ không chỉ làm cho vấn đề an toàn phức tạp hơn nhiều mà còn khiến cho vấn đề này trở nên thiết yếu hơn nữa. Kiến trúc mạng lõi đã thay đổi từ môi trường máy tính độc lập sang môi trường tính toán phân tán làm độ phức tạp tăng lên theo cấp số nhân. Mặc dù việc kết nối với Internet tăng thêm nhiều chức năng và dịch vụ cho người dùng và nâng cao khả năng thể hiện hình ảnh của cơ quan/tổ chức với thế giới Internet song việc kết nối này mở ra vô số các rủi ro an toàn tiềm ẩn.

Ngày nay, đa số các cơ quan/tổ chức không thể hoạt động nếu không có máy tính và khả năng xử lý. Máy tính đã được tích hợp vào công việc của cơ quan/tổ chức cũng như cá nhân. Hầu hết các cơ quan/tổ chức đã nhận ra rằng dữ liệu của họ là tài sản cần được bảo vệ cũng như các tòa nhà, thiết bị máy móc và các tài sản vật chất khác của họ. Trong hầu hết các trường hợp, dữ liệu nhạy cảm của tổ chức thậm chí còn quan trọng hơn các tài sản vật chất này.

Vì mạng và môi trường hoạt động thay đổi nên cần có an ninh. An ninh không chỉ là các biện pháp kiểm soát kỹ thuật đưa ra để bảo vệ tài sản của cơ quan/tổ chức; các biện pháp kiểm soát này phải được quản lý và phần quan trọng của việc đảm bảo an toàn là quản lý các hành động của người dùng và các quy trình mà họ phải thực hiện.

Thực tiễn quản lý an toàn tập trung vào việc bảo vệ liên tục tài sản và tài nguyên của cơ quan/tổ chức. Quản lý an toàn bao gồm tất cả các hoạt động cần thiết để giữ cho một chương trình bảo mật hoạt động và phát triển. Việc quản lý này bao gồm quản lý rủi ro, lập tài liệu, triển khai và quản lý kiểm soát an toàn, quy trình và thủ tục, an ninh nhân sự, kiểm toán và đào tạo nâng cao nhận thức bảo mật liên tục.

Việc phân tích rủi ro xác định các tài sản quan trọng, phát hiện ra các mối đe dọa gây ra nguy cơ cho các tài sản đó và việc phân tích được sử dụng để ước tính thiệt hại có thể và tổn thất tiềm ẩn mà cơ quan/tổ chức có thể chịu đựng. Phân tích rủi ro giúp quản lý xây dựng ngân sách cần thiết để bảo vệ tài sản được xác định khỏi các mối đe dọa được xác định và phát triển các chính sách an toàn giúp định hướng cho các hoạt động an ninh.

Các biện pháp kiểm soát được xác định, triển khai và duy trì để giữ rủi ro an toàn của tổ chức ở mức có thể chấp nhận được. Các biện pháp kiểm soát có thể bao gồm:

- Kiểm soát quản trị: yêu cầu về an toàn, quản lý rủi ro, đào tạo
- Kiểm soát kỹ thuật : phần cứng hay phần mềm như tường lửa, kiểm soát truy nhập, phát hiện xâm nhập
- Kiểm soát vật lý: biện pháp bảo vệ các phương tiện, tài sản như nhà xưởng, phòng ốc

Bên cạnh đó, giáo dục và nâng cao nhận thức an toàn đưa thông tin về các biện pháp kiểm soát đến từng nhân viên trong cơ quan/tổ chức để mọi người được thông báo đầy đủ và có thể dễ dàng làm việc hướng tới các mục tiêu an ninh tương tự.

Tóm lại, việc quản lý an toàn thông tin mô tả các biện pháp kiểm soát cần thiết triển khai để đảm bảo quản lý được các rủi ro về mất, lạm dụng, lộ bí mật hay hư hỏng các thông tin và tài sản hạ tầng thông tin của cơ quan/tổ chức. Hệ thống quản lý an toàn thông tin là một phần của hệ thống quản lý, dựa trên các tiếp cận rủi ro kinh doanh/công việc để thiết lập, triển khai, vận hành, giám sát, xem xét, duy trì và cải thiện an toàn thông tin.

## 1.5 Các nguyên tắc quản lý an toàn thông tin

Quản trị an toàn là tập hợp các thực tiễn liên quan đến hỗ trợ, xác định và chỉ đạo các nỗ lực an toàn của cơ quan/tổ chức. Quản trị an toàn có liên quan chặt chẽ và thường gắn bó với quản trị cơ quan/tổ chức và CNTT. Một số khía cạnh quản lý tác động lên cơ quan/tổ chức do yêu cầu phù hợp với quy định về pháp luật, ngược lại số khác ảnh hưởng bởi các hướng dẫn quy chuẩn công nghiệp hay yêu cầu bản quyền. Với công ty lớn, xuyên quốc gia thì vấn đề trở nên phức tạp hơn nhiều.

Toàn bộ công việc quản lý an toàn thỉnh thoảng cần phải được đánh giá và kiểm chứng. Vấn đề an toàn không nên và không thể chỉ coi là nhiệm vụ chuyên biệt của CNTT. Vấn đề an toàn ảnh hưởng tới mọi khía cạnh của cơ quan/tổ chức, do vậy nhân viên CNTT không thể xử lý hết được.

Các nguyên tắc cơ bản trong quản lý an toàn thông tin:

- Xây dựng các chức năng an toàn hướng tới mục tiêu, nhiệm vụ, kết quả và chiến lược của cơ quan/tổ chức
- Xây dựng các quy trình tổ chức
- Xây dựng vai trò và trách nhiệm với an toàn
- Xây dựng khung kiểm tra/kiểm soát
- Cần mẫn và cẩn trọng thích đáng

### 1.5.1 *Xây dựng chức năng an toàn*

Việc lập kế hoạch quản lý an toàn cần điều chỉnh các chức năng an ninh/an toàn phù hợp với mục tiêu, nhiệm vụ, kết quả và chiến lược của cơ quan/tổ chức. Điều này bao gồm việc thiết kế và triển khai an toàn dựa trên các nguyên tắc hoạt động hay kinh doanh của cơ quan/tổ chức, các ràng buộc về kinh phí và tính sẵn có của nguồn lực.

Cách tiếp cận hiệu quả nhất để xử lý việc lập kế hoạch quản lý an toàn là từ trên xuống. Bộ phận đầu não và ban lãnh đạo chịu trách nhiệm khởi xướng và xây dựng các chính sách cho cơ quan. Các phòng ban quản lý hoàn chỉnh các chính sách này thành các hướng dẫn, quy định, thủ tục và tiêu chuẩn. Chuyên viên CNTT và nhân viên quản lý chịu trách nhiệm triển khai các cấu hình phù hợp với các tài liệu về quản lý an toàn. Cuối cùng người dùng cuối cần tuân thủ với yêu cầu an toàn cơ sở của cơ quan/tổ chức.

Việc xây dựng các kế hoạch quản lý phù hợp với các mục tiêu chiến lược, trung hạn và ngắn hạn của cơ quan/tổ chức.

### 1.5.2 *Các quy trình tổ chức*

Quản trị an toàn cần hướng tới mọi khía cạnh của cơ quan/tổ chức bao gồm các quy trình tổ chức của các việc tiếp nhận, loại trừ. Cụ thể:

- Việc tiếp nhận là tăng mức độ rủi ro như lộ thông tin, mất dữ liệu, hay hệ thống không hoạt động
- Việc loại trừ dưới bất kỳ dạng nào như thanh lý tài sản hay cắt giảm nhân sự là thời điểm làm tăng rủi ro. Tài sản cần phải được tẩy sạch để ngừa rò rỉ thông tin. Nhân viên trước khi thôi việc cần được phỏng vấn và đánh giá lại các thỏa thuận và ràng buộc trong hợp đồng.

Quản trị an toàn cần được điều hành bởi hội đồng quản trị hay ban lãnh đạo nhằm để theo dõi và định hướng các hoạt động về an toàn cho cơ quan/tổ chức để thực hiện nhiệm vụ:

- *Quản lý và kiểm soát thay đổi*. Các thay đổi trong môi trường an toàn có thể dẫn đến các lỗ hổng, trùng lặp, sai lệch mục tiêu, và thiếu sót dẫn đến các lỗ hổng mới. Cách đối phó duy nhất là quản lý thay đổi một cách có hệ thống

thông qua việc lập kế hoạch chi tiết, kiểm tra, theo dõi, ghi nhật ký các hoạt động liên quan tới các cơ chế và công cụ an toàn.

Mục tiêu quan trọng nhất của việc quản lý này là đảm bảo không một thay đổi nào làm suy giảm hay mất tác dụng của hệ thống an toàn.

- Phân loại dữ liệu. Việc phân loại dữ liệu là cách thức chủ yếu để bảo vệ dữ liệu dựa trên yêu cầu về tính bí mật, nhạy cảm của chúng. Sẽ không hiệu quả khi bảo vệ tất cả các dữ liệu đều như nhau. Việc phân loại giúp xây dựng mức độ nỗ lực, khi phí và nguồn lực cần phân bổ để bảo vệ dữ liệu và các biện pháp kiểm soát truy nhập tới nó.

  Quá trình phân loại dữ liệu sắp xếp các mục, đối tượng, và chủ thể ... vào trong các nhóm tương tự nhau dựa trên các yếu tố như giá trị, chi phí, rủi ro, đặc quyền ...

### 1.5.3 *Vai trò và trách nhiệm an toàn*

Vai trò an toàn là phần việc mà mỗi cá nhân tham gia vào trong kế hoạch tổng thể về quản trị và triển khai an toàn bên trong cơ quan/tổ chức. Các vai trò an toàn không nhất thiết được mô tả trong nhiệm vụ do chúng không hoàn toàn cố định hay tách biệt.

Nắm vững vai trò an toàn/an ninh giúp mọi người xây dựng cơ chế hỗ trợ và liên lạc bên trong cơ quan/tổ chức. Cơ chế này cho phép triển khai và thực hiện (bắt buộc) các chính sách an toàn. Các vai trò tiêu biểu: quản lý cao cấp, chuyên viên an toàn, chủ dữ liệu, bảo vệ dữ liệu, người dùng, kiểm toán/giám sát...

Việc phân định các vai trò có tác dụng quan trọng với môi trường được bảo vệ và hữu ích cho việc xác định trách nhiệm và liên đới cũng như xây dựng phân cấp quản lý.

### 1.5.4 *Hệ thống kiểm soát*

Xây dựng hệ thống an toàn cho cơ quan/tổ chức thường cần làm nhiều việc hơn là vạch ra các ý tưởng. Việc quan trọng đầu tiên với quản lý an toàn là xem xét hệ thống kiểm soát (*control framework*) hay các giải pháp an toàn một cách tổng thể. Thay vì tự xây dựng, cơ quan/tổ chức có thể xem xét các giải pháp/hệ thống kiểm soát an toàn có sẵn được khuyến nghị hay đề xuất bởi các tổ chức tiêu chuẩn hay hiệp hội nghề nghiệp mà phù hợp với nhu cầu của riêng mình. Có thể kể tên một số khung kiểm soát tiêu biểu như COBIT (*Control Objectives for Information and related Technology)*, ISO 27001/2, NIST 800-53.

COBIT thường được các giám đốc điều hành sử dụng để thực hiện thành công các chính sách và thủ tục quan trọng của tổ chức. Ngoài ra, nó thường được sử dụng để kết hợp các biện pháp kiểm soát, các vấn đề kỹ thuật và các rủi ro trong một tổ chức. COBIT được quản lý bởi ISACA (Hiệp hội Kiểm toán và Kiểm soát Hệ thống Thông tin) và duy trì cập nhật tiêu chuẩn và ngang hàng với công nghệ hiện tại. Nó là một tiêu chuẩn được chấp nhận trên toàn cầu và hàm chứa nhiều hơn là phạm vi an toàn thông tin mà các tiêu

chuẩn khác được giới hạn. Mặt khác COBIT có thể dễ dàng hơn khi triển khai một phần mà không yêu cầu phân tích và cam kết toàn diện của cơ quan/tổ chức.

ISO 27001/2 là tiêu chuẩn rất được tôn trọng và được biết đến rộng rãi. Bên cạnh đó chúng được công nhận và hiểu bởi những người quen thuộc với các tiêu chuẩn ISO. Tiêu chuẩn này cho phép các nhà quản lý hệ thống xác định và giảm thiểu các khoảng trống và chồng chéo trong vùng tác dụng của tiêu chuẩn này.

NIST bao gồm tất cả các bước trong quản lý rủi ro đề cập đến việc lựa chọn các biện pháp kiểm soát an toàn và được các tổ chức liên bang của Hoa Kỳ sử dụng để đáp ứng các yêu cầu của hệ thống quản lý an toàn thông tin. Mức độ chi tiết trong việc thực hiện dựa trên NIST là đáng kể. Nếu cơ quan/tổ chức không muốn dành thời gian vào việc tùy chỉnh khung kiểm soát cụ thể của họ thì có thể sử dụng NIST với giả định mức độ chi tiết phù hợp các mục tiêu của nó.

### 1.5.5 *Cần mẫn và cẩn trọng thích đáng*

Cẩn trọng giúp bảo vệ lợi ích của cơ quan/tổ chức còn cần mẫn giúp duy trình các nỗ lực bảo vệ. Việc cẩn trọng thể hiện qua việc phát triển các cơ chế an toàn chính tắc (*formal security*) bao gồm các chính sách, tiêu chuẩn, hướng dẫn và các thủ tục. Việc cần mẫn thực thi các cơ chế an toàn này lên hạ tầng CNTT một cách đầy đủ.

An toàn về hoạt động là việc duy trì liên tục việc cẩn trọng và cần mẫn bởi tất cả các bên trong cơ quan. Như vậy giúp loại trừ các bất cẩn hay thiếu sót khi có sự cố an toàn.

## 1.6 Chính sách và luật pháp an toàn thông tin

### 1.6.1 *Chính sách an toàn*

Vấn đề trước tiên của việc quản lý an toàn là chính sách an toàn. Chính sách này là tài liệu xác định phạm vi bảo mật cần thiết của cơ quan/tổ chức và thảo luận về các tài sản cần bảo vệ cũng như các giải pháp an toàn để đảm bảo mức độ bảo vệ cần thiết. Chính sách an toàn cho biết một cách tổng quát về nhu cầu đảm bảo an toàn của cơ quan/tổ chức. Các chính sách này định nghĩa các mục tiêu an toàn chính và vạch ra khung bảo mật của cơ quan/tổ chức.

Chính sách an toàn cần phác thảo một cách khái quát các mục tiêu và thực tiễn an ninh cần được sử dụng để bảo vệ lợi ích quan trọng của cơ quan/tổ chức. Bên cạnh đó, chính sách này thảo luận về tầm quan trọng của an ninh đối với mọi khía cạnh của hoạt động hay công việc thường xuyên và tầm quan trọng của sự hỗ trợ của các cán bộ cấp cao để thực hiện an ninh. Chính sách an toàn được sử dụng để phân công trách nhiệm, xác định vai trò, chỉ định các yêu cầu kiểm toán, phác thảo quy trình thực thi, cho biết các yêu cầu tuân thủ và xác định các mức độ rủi ro có thể chấp nhận được.

### 1.6.2 *Đạo đức và luật pháp*

Ở góc độ xã hội, thông thường con người chọn lọc từ bỏ một số khía cạnh tự do cá nhân để đảm bảo trật tự xã hội. Các quy định với các thành viên trong cộng đồng được tạo ra để cân bằng các quyền tự khẳng định bản thân đối chọi với các yêu cầu của toàn thể cộng đồng được coi là luật. Luật pháp là các quy định bắt buộc hay cấm một số hành vi nhất định; chúng được xây dựng dựa trên đạo đức mà xác định các hành vi chấp nhận được trong xã hội. Luật pháp đi kèm với cơ quan quyền lực để quản lý và thực thi các quy định của mình.

Đạo đức được phát triển dựa trên cơ sở các tập tục văn hóa như thái độ đạo đức hay thói quen của một nhóm cụ thể. Thông thường, đạo đức có tính ràng buộc thấp hơn so với luật pháp ở khía cạnh thực hiện. Việc vi phạm các quy định của luật pháp thường được các cơ quan thực thi luật pháp theo dõi, ngăn chặn và chấm dứt các hành vi này của cá nhân hay tổ chức. Xử phạt hành vi vi phạm như bồi thường hay nộp phạt được coi là đủ để khôi phục tư cách của cá nhân hay tổ chức trong các hoạt động tiếp theo. Tuy nhiên, việc xử lý các hành động vi phạm đạo đức không đơn giản như vậy. Các hành vi vi phạm các giá trị đạo đức được cộng đồng thừa nhận có ảnh hưởng rất nghiêm trọng và lâu dài đến các cá nhân hay tổ chức vi phạm. Các cơ quan/tổ chức phải dành rất nhiều thời gian và công sức để khôi phục niềm tin của cộng đồng.

Hoạt động trong lĩnh vực an toàn thông tin, điều quan trọng với mỗi cá nhân cũng như cơ quan/tổ chức là hiểu được vai trò và ảnh hưởng của luật pháp, các quy định và các giá trị được cộng đồng và xã hội trân trọng cũng như việc tuân thủ các yêu cầu này tới các hoạt động của cơ quan/tổ chức. Các yêu cầu và ràng buộc này tác động đến các hoạt động cụ thể cũng như việc đề ra các chính sách an toàn như:

- Bảo vệ hoạt động của cơ quan/tổ chức
- Thiết kế hệ thống CNTT và các ứng dụng mới
- Quyết định thời hạn lưu giữ dữ liệu
- Phương pháp mã hóa dữ liệu nhạy cảm
- ....

Các cơ quan/tổ chức nghề nghiệp lớn thường xây dựng các quy định nghề nghiệp hay quy định về đạo đức để yêu cầu các thành viên tuân thủ để thể hiện nỗ lực và cống hiến tới sự phát triển bền vững và an toàn của cộng đồng như, Có thể kể đến các tổ chức như:

- Hiệp hội an toàn hệ thống thông tin (Information Systems Security Association) *www.issa.org*
- Hiệp hội máy tính (Association of Computing Machinery) *www.acm.org*
- Tập đoàn chứng nhận an toàn hệ thống thông tin quốc tế ( International Information Systems Security Certification Consortium) *www.isc2.org*
- Hiệp hội an toàn thông tin Việt Nam *VNISA* vnisa.org.vn

## 1.7 Câu hỏi ôn tập

1. Trình bày và phân tích khái niệm về an toàn thông tin.
2. Nêu và phân tích tương quan giữa các các khái niệm cơ bản: tài sản, tấn công, biện pháp, rủi ro, đe dọa.
3. Giải thích sự tác động của các yêu cầu an toàn khác bên cạnh các thuộc tính về bí mật, sẵn dùng, và toàn vẹn lên việc đảm bảo an toàn của hệ thống thông tin.
4. Giải thích khái niệm chương trình an toàn.
5. Tại sao cần có khung an toàn?
6. Nếu phải xây dựng phần mềm truy vết tiếp xúc gần thông qua công nghệ Bluetooth, mục tiêu an toàn của phần mềm sẽ gồm những yêu cầu nào? Đề xuất khung an toàn cho chương trình này.
7. Giới thiệu cách thức xây dựng kiến trúc doanh nghiệp và khung an toàn cho cơ quan/tổ chức.
8. Nêu và phân tích các khái niệm về quản trị, chính sách, luật pháp về an toàn thông tin.
9. Phân tích ảnh hưởng của đạo đức, chính sách và luật pháp tới hành vi sử dụng máy tính hay hệ thống mạng.
10. Phân tích ảnh hưởng qua lại giữa đạo đức, chính sách và luật pháp trong việc điều chỉnh hành vi sử dụng máy tính.

# CHƯƠNG 2. XÂY DỰNG KẾ HOẠCH AN TOÀN

Chương này giới thiệu các vấn đề cơ bản trong việc xây dựng và triển khai các kế hoạch an toàn cho cơ quan/tổ chức. Kế hoạch an toàn đóng vai trò rất quan trọng trong việc đảm bảo các mục tiêu an toàn được đảm bảo bởi các biện pháp tổ chức quản lý an toàn phù hợp. Ngoài ra, trình bày cách tiếp cận cơ bản cho việc phân loại mức độ quan tâm với các tài sản và hệ thống được quản lý cũng như mô hình mối đe dọa với hệ thống ứng dụng dựa trên Internet.

## 2.1 Giới thiệu

Thật khó để nói quá mức độ thiết yếu của việc xây dựng kế hoạch an toàn đối với hoạt động kinh doanh và quản lý cơ quan/tổ chức. Trong bối cảnh liên tục có những hạn chế về nguồn lực, cả nhân lực và tài chính, việc lập kế hoạch tốt cho phép tổ chức tận dụng tối đa các tài nguyên hiện có. Tuy nhiên, một số cơ quan/tổ chức dành quá nhiều thời gian, tiền bạc và công sức của con người vào việc xây dựng kế hoạch trong khi lợi ích thu về quá ít để biện minh cho khoản đầu tư của họ. Mỗi cơ quan/tổ chức phải cân bằng giữa lợi ích của mức độ nỗ lực xây dựng  kế hoạch đã chọn so với chi phí của nỗ lực đó.

Khi lập kế hoạch, các thành viên của nhóm an toàn thông tin  sử dụng các quy trình và phương pháp tương tự mà nhóm quản lý và quản lý công nghệ thông tin nói chung sử dụng. Vì nhóm an toàn thông tin tìm cách tác động đến toàn bộ cơ quan/tổ chức, người lập kế hoạch an toàn thông tin hiệu quả phải biết cách hoạt động của quá trình lập kế hoạch của cơ quan/tổ chức để việc tham gia vào quá trình này có thể mang lại kết quả có thể đo đếm được.

Lập kế hoạch là phương tiện chủ đạo để quản lý các nguồn lực trong các cơ quan/tổ chức hiện đại. Nó đòi hỏi việc liệt kê một chuỗi các hành động nhằm đạt được các mục tiêu cụ thể trong một khoảng thời gian xác định, và sau đó kiểm soát việc thực hiện các bước này. Lập kế hoạch cung cấp định hướng cho tương lai của tổ chức. Nếu không có kế hoạch cụ thể và chi tiết, các đơn vị thành viên sẽ cố gắng đạt được các mục tiêu một cách độc lập, với mỗi đơn vị được dẫn dắn bởi các sáng kiến và ý tưởng của riêng mình. Các nỗ lực không có sự phối hợp như vậy sẽ không chỉ không đạt được các mục tiêu mà còn dẫn đến việc sử dụng các nguồn lực một cách kém hiệu quả.

Lập kế hoạch tổ chức, khi được tiến hành bởi các bộ phận khác nhau của tổ chức, cung cấp một kịch bản thống nhất nhằm tăng hiệu quả và giảm lãng phí và trùng lặp nỗ lực của từng đơn vị thành viên trong các nhóm riêng lẻ mà họ quan tâm. Việc lập kế hoạch tổ chức nên sử dụng một quy trình từ trên xuống trong đó ban lãnh đạo của cơ quan/tổ chức chọn hướng đi và các sáng kiến mà toàn bộ cơ quan/tổ chức nên theo đuổi.

Ban đầu, kế hoạch tổ chức chứa ít mục tiêu chi tiết cụ thể; thay vào đó, nó vạch ra các mục tiêu chung.

Mục tiêu chính của quá trình lập kế hoạch tổ chức là việc tạo ra các kế hoạch chi tiết nghĩa là, các định hướng có hệ thống về cách đáp ứng các mục tiêu của cơ quan/tổ chức. Nhiệm vụ này được thực hiện với một quá trình bắt đầu với cái khái quát và kết thúc bằng cái cụ thể.

## 2.2 Lập kế hoạch chiến lược

Hoạch định chiến lược đưa ra định hướng dài hạn mà tổ chức sẽ thực hiện. Chiến lược này dẫn dắt các nỗ lực của cơ quan/tổ chức và tập trung nguồn lực vào các mục tiêu cụ thể, được xác định rõ ràng trong bối cảnh môi trường luôn thay đổi. Các kế hoạch chiến lược được hình thành ở các cấp cao nhất của cơ quan/tổ chức được chuyển thành các kế hoạch chiến lược cụ thể hơn cho các tầng quản lý trung gian. Các kế hoạch này sau đó được chuyển thành kế hoạch sách lược cho các nhà quản lý giám sát và cuối cùng cung cấp định hướng cho các kế hoạch hoạt động do các thành viên chịu trách nhiệm quản lý của cơ quan/tổ chức đảm nhận. Cách tiếp cận nhiều lớp này bao gồm hai mục tiêu chính: chiến lược chung và hoạch định chiến lược tổng thể. Thứ nhất, chiến lược chung được chuyển thành chiến lược cụ thể; thứ hai, hoạch định chiến lược tổng thể được chuyển thành kế hoạch sách lược và hoạt động cấp thấp hơn.

Sau khi kế hoạch chiến lược tổng thể của tổ chức được chuyển thành các mục tiêu chiến lược cho từng bộ phận hoặc hoạt động chính, bước tiếp theo là chuyển các chiến lược này thành các nhiệm vụ với các mục tiêu cụ thể, có thể đo đếm, có thể đạt được và có thời hạn. Sau đó, hoạch định chiến lược bắt đầu chuyển đổi từ các tuyên bố chung chung, sâu rộng sang các mục tiêu cụ thể và áp dụng hơn. Kế hoạch chiến lược được sử dụng để tạo ra các kế hoạch sách lược, sau đó được sử dụng để phát triển các kế hoạch hoạt động.

Lập kế hoạch sách lược có trọng tâm ngắn hạn hơn lập kế hoạch chiến lược - thường là từ một đến ba năm. Nó chia nhỏ từng mục tiêu chiến lược có thể áp dụng thành một loạt các mục tiêu gia tăng. Mỗi mục tiêu phải cụ thể và lý tưởng là sẽ có kết quả trong ngắn hạn.

Lập ngân sách, phân bổ nguồn lực và nhân sự là những thành phần quan trọng của kế hoạch sách lược. Mặc dù các thành phần này có thể được thảo luận chung chung ở cấp độ hoạch định chiến lược, nhưng chúng rất quan trọng ở cấp độ sách lược vì chúng phải được thực hiện trước khi kế hoạch sách lược có thể được chuyển thành kế hoạch thực thi. Kế hoạch sách lược thường bao gồm lên kế hoạch dự án và lập tài liệu thu nhận nguồn lực (chẳng hạn như thông số kỹ thuật của sản phẩm), ngân sách dự án, đánh giá dự án và báo cáo hàng tháng và hàng năm.

Ban lãnh đạo về an toàn thông tin và các nhà quản lý an toàn sử dụng kế hoạch sách lược để tổ chức, sắp xếp thứ tự ưu tiên và thu thập các nguồn lực cần thiết cho các dự án lớn và hỗ trợ cho kế hoạch chiến lược tổng thể.

Các nhà quản lý và nhân viên sử dụng các kế hoạch thực thi, được bắt nguồn từ các kế hoạch sách lược, để tổ chức thực hiện nhiệm vụ liên tục hàng ngày. Kế hoạch thực thi bao gồm các hoạt động phối hợp được xác định rõ ràng bao gồm các ranh giới của bộ phận, các yêu cầu về thông tin liên lạc, các cuộc họp hàng tuần, tóm tắt, báo cáo tiến độ và các nhiệm vụ liên quan. Các kế hoạch này được thiết kế cẩn thận để phản ánh cơ cấu tổ chức, với mỗi đơn vị thành viên, bộ phận hoặc nhóm dự án thực hiện các thành phần báo cáo và lập kế hoạch hoạt động của riêng mình. Thông tin liên lạc và phản hồi thường xuyên từ các nhóm tới các nhà quản lý dự án và/hoặc trưởng nhóm và sau đó lên các cấp quản lý khác nhau sẽ làm cho quá trình lập kế hoạch nói chung dễ quản lý và thành công hơn.

## 2.3 Các nhiệm vụ chính

Để thực hiện quản lý an toàn thông tin một cách hiệu quả cần thực hiện nhiều biện pháp khác nhau. Dưới đây trình bày các nhiệm vụ tiêu biểu.

- *Xây dựng chính sách.* Việc xây dựng chính sách quyết định sống còn đến việc đảm bảo an toàn cho cơ quan/tổ chức. Các chính sách này giúp xác định tính đúng đắn của các mục tiêu an toàn đề ra cũng như sự phù hợp của các mục tiêu an toàn với các công việc và nhiệm vụ của cơ quan/tổ chức cần thực hiện để tồn tại và phát triển.
- *Lập kế hoạch xây dựng khung an toàn/chương trình an toàn*. Việc xem xét thực tiễn hoạt động và các biện pháp kiểm soát sẵn có trong các khuyến nghị và các tiêu chuẩn cho phép cơ quan/tổ chức lựa chọn được cách thức phù hợp để đảm bảo các nhiệm vụ và công việc của mình được bảo vệ một cách phù hợp và cân bằng giữa yêu cầu về an toàn và các chi phí cho các biện pháp bảo vệ.
- *Đánh giá kết quả (hiệu năng)* cho phép xác định và kiểm chứng tính đúng đắn và hiệu quả của các biện pháp an toàn được triển khai. Bên cạnh đó việc đánh giá cho phép xác định các lỗ hổng xuất hiện trong quá trình hoạt động và vận hành của cơ quan/tổ chức.
- *Quản lý thay đổi* trong quá trình hoạt động của cơ quan/tổ chức giúp việc ứng phó và kiểm soát các biến động được tốt hơn. Điều quan trọng hơn là các biến động này không làm nảy sinh các lỗ hổng mới hay vấn đề với an toàn thông tin. Các thay đổi này rất đa dạng có thể xuất phát từ việc thay đổi mục tiêu của cơ quan/tổ chức, biến động về công nghệ, thay đổi về chính sách hay quy định của nhà nước hay các tổ chức đối tác quốc tế.

- *Quản lý rủi ro* nhằm xác định, đánh giá các vấn đề an toàn với các tài sản cần bảo vệ của cơ quan/tổ chức cũng như biện pháp kiểm soát để đối phó với trường hợp hệ thống bị xâm phạm an toàn. Việc quản lý rủi ro cung cấp cái nhìn chi tiết về các mối đe dọa, mức độ tác động và chi phí để khắc phục mối đe dọa cho phép cơ quan/tổ chức xử lý một cách hiệu quả các lỗ hổng trong quá trình hoạt động của mình.
- *Quản lý vận hành an toàn* hướng tới việc triển khai và thực hiện một cách đầy đủ các biện pháp kiểm soát với hệ thống thông tin của cơ quan/tổ chức.
- *Xử lý sự cố* đối phó với trường hợp hệ thống bị xâm phạm các yêu cầu an toàn. Mục tiêu quan trọng của việc xử lý sự cố là đảm bảo việc hoạt động tối thiểu của cơ quan/tổ chức trong quá trình xảy ra sự cố, khắc phục và vượt qua các hậu quả của sự cố giúp cho cơ quan/tổ chức có thể tiếp tục hoạt động sau này.
- *Đào tạo nâng cao nhận thức an toàn* nhằm cung cấp thông tin đầy đủ và đúng đắn về các vấn đề an toàn thông tin cũng như các biện pháp kiểm soát cần thiết tới mọi người dùng và nhân viên của cơ quan/tổ chức. Việc này không chỉ giới hạn ở các chuyên gia và nhân viên chịu trách nhiệm về an toàn thông tin. Trên thực tế, mọi người đều có trách nhiệm hiểu biết và thực thi một cách đầy đủ các yêu cầu và các biện pháp an toàn.

## 2.4 Tổ chức quản lý an toàn thông tin

Việc quản lý an toàn thông tin là một trách nhiệm hoạch định chiến lược mà tầm quan trọng của nó đã tăng lên trong những năm gần đây. Tuy nhiên, an toàn thông tin thường được coi là một vấn đề kỹ thuật trong khi trên thực tế, nó lại là một vấn đề quản lý. Để bảo mật tài sản thông tin, ban lãnh đạo của cơ quan/tổ chức phải tích hợp các thông lệ an toàn thông tin vào cấu trúc của tổ chức, mở rộng các chính sách và kiểm soát quản lý cơ quan/tổ chức để chứa đựng các mục tiêu của quy trình an toàn thông tin.

Các mục tiêu của an toàn thông tin phải được đề cập ở cấp cao nhất của đội ngũ quản lý để có hiệu quả và đưa ra cách thức tiếp cận bền vững. Khi các chương trình an toàn được thiết kế và quản lý như một chuyên môn kỹ thuật trong bộ phận CNTT, chúng ít có hiệu quả hơn. Cái nhìn rộng hơn về an toàn thông tin bao gồm tất cả các tài sản thông tin của một tổ chức, bao gồm cả tri thức đang được quản lý bởi các tài sản CNTT đó. Những hàng hóa có giá trị này phải được bảo vệ bất kể thông tin được xử lý, lưu trữ hoặc truyền đi như thế nào và với sự hiểu biết thấu đáo về rủi ro và lợi ích của tài sản thông tin.

Việc xác định rõ ràng vai trò và trách nhiệm trong việc quản lý an toàn thông tin quyết định tính hiệu quả của các biện pháp cũng như hiệu lực của các chính sách an toàn thông tin. Thực tế cho thấy, số lượng đáng kể các lãnh đạo cấp cao không thực sự hiểu rõ các rủi ro về an toàn cũng như trách nhiệm của họ với vấn đề an toàn hệ thống thông tin. Kết quả rất khó để có được sự quan tâm thích đáng tới các vấn đề an toàn cũng như các sáng kiến thúc đẩy an toàn thông tin.

Tổ chức hiệu quả với quản trị an toàn thông tin cần liên kết các mức quản lý của cơ quan/tổ chức:

- Ban lãnh đạo
- Quản lý cấp cao
- Ban điều hành về an toàn
- Giám đốc an toàn thông tin

Ban lãnh đạo chịu trách nhiệm xác lập các định hướng chiến lược và đảm bảo các rủi ro được quản lý một cách thích đáng cũng như sử dụng các tài nguyên và đánh giá kết quả (hiệu năng). Quản lý cấp cao hỗ trợ tích cực các sáng kiến từ ban quản lý. Nếu không có sự hỗ trợ này các quản lý về an toàn khó vượt qua trở ngại từ các cấp quản lý khác để thực hiện hiệu quả các chính sách an toàn.

Việc tổ chức ban điều hành về an toàn hợp lý có tác dụng cải thiện hiệu quả của quản trị an toàn thông tin. Những người tham gia lý tưởng là các đại diện cấp cao chịu trách nhiệm quản lý hay vận hành cơ quan/tổ chức. Điều này giúp nhanh chóng xác định và ưu tiên các rủi ro mới xuất hiện và kênh thông tin quan trọng để phổ biến các thông tin quan trọng liên quan đến an toàn.

Do thay đổi về nhận thức vấn đề an toàn, các quản lý về an toàn thông tin được tăng trách nhiệm và quyền lực trong nhiều lĩnh vực. Một số cơ quan xây dựng chức danh giám đốc về an toàn thông tin phụ trách:

- Xây dựng chi tiết các chiến lược hay chính sách an toàn thông tin
- Tư vấn cho lãnh đạo cấp cao về các vấn đề liên quan đến an toàn cũng như báo cáo trực tiếp lên lãnh đạo cấp cao và ban lãnh đạo
- Quản lý các chương trình an toàn và việc triển khai
- Trao đổi với các lãnh đạo bộ phận khác để đảm bảo an toàn thông tin trên tất cả các bộ phận

Ban kiểm tra/kiểm toán phải được chỉ định bởi ban lãnh đạo để giúp họ xem xét và đánh giá các hoạt động nội bộ của công ty, hệ thống kiểm toán nội bộ và tính minh bạch và chính xác của báo cáo tài chính để các khách hàng và đối tác tiếp tục tin tưởng vào cơ quan/tổ chức. Mục tiêu của ban này là cung cấp thông tin độc lập và cởi mở giữa ban lãnh đạo, quản lý của công ty, kiểm toán nội bộ và kiểm toán viên bên ngoài. Khi có sự cố vai trò của ủy ban kiểm toán đã chuyển từ theo dõi, giám sát và tư vấn sang thực thi và đảm bảo trách nhiệm của tất cả các thành viên liên quan.

Các vai trò và nhiệm vụ tiêu biểu về quản lý an toàn gồm có:

- *Quản lý cấp cao* là người chịu trách nhiệm tối cao về an toàn được duy trì bởi cơ quan/tổ chức và là người quan tâm nhất đến việc bảo vệ tài sản. Người quản lý cấp cao phải ký vào tất cả các văn bản về chính sách. Trên thực tế, tất cả các hoạt động phải được người quản lý cấp cao chấp thuận và phê duyệt trước khi chúng có thể được thực hiện. Không có chính sách an toàn hiệu quả

nếu người quản lý cấp cao không cho phép và hỗ trợ chính sách đó. Người quản lý cấp cao là người chịu trách nhiệm về thành công hoặc thất bại chung của giải pháp an toàn và chịu trách nhiệm thực hiện việc theo dõi và thẩm định cẩn thận trong việc thiết lập an toàn. Mặc dù các nhà quản lý cấp cao chịu trách nhiệm cuối cùng về an toàn, họ hiếm khi thực hiện các giải pháp bảo mật. Trong hầu hết các trường hợp, trách nhiệm đó được giao cho các chuyên gia an ninh trong tổ chức.

- *Chuyên gia an ninh* hoặc vai trò của đội phản ứng sự cố máy tính được giao cho một nhóm, hệ thống và kỹ sư an toàn có kinh nghiệm và được đào tạo chịu trách nhiệm tuân thủ các chỉ thị do quản lý cấp cao uỷ nhiệm. Chuyên gia bảo mật có trách nhiệm chức năng về an toàn bao gồm viết chính sách bảo mật và triển khai nó. Vai trò của chuyên gia bảo mật có thể được gắn nhãn là vai trò chức năng hệ thống thông tin/CNTT. Vai trò chuyên môn bảo mật thường được gán cho một nhóm chịu trách nhiệm thiết kế và triển khai các giải pháp an toàn dựa trên chính sách an toàn được phê duyệt. Các chuyên gia bảo mật không phải là người ra quyết định mà họ là những người thực hiện. Tất cả các quyết định phải được để lại cho người quản lý cấp cao.
- *Chủ sở hữu dữ liệu*. Vai trò này được gán cho người chịu trách nhiệm phân loại thông tin cho việc triển khai và bảo vệ trong giải pháp an toàn. Chủ sở hữu dữ liệu thường là người quản lý cấp cao, người chịu trách nhiệm cuối cùng về bảo vệ dữ liệu. Tuy nhiên, chủ sở hữu dữ liệu thường ủy quyền trách nhiệm của các nhiệm vụ quản lý dữ liệu thực tế cho người quản lý dữ liệu.
- *Giám sát dữ liệu.* Vai trò giám sát dữ liệu được gán cho người dùng chịu trách nhiệm thực hiện việc bảo vệ theo quy định được xác định bởi chính sách an toàn và quản lý cấp cao. Người quản lý dữ liệu thực hiện tất cả các hoạt động cần thiết để đảm bảo việc bảo vệ đầy đủ cho bộ ba bảo mật, toàn vẹn và sẵn dùng của dữ liệu và để đáp ứng các yêu cầu và trách nhiệm được giao từ cấp trên. Các hoạt động này có thể bao gồm thực hiện và thử nghiệm các bản sao lưu, xác thực tính toàn vẹn dữ liệu, triển khai các giải pháp bảo mật và quản lý lưu trữ dữ liệu dựa trên phân loại.
- *Người dùng.* Vai trò người dùng (người dùng cuối hoặc người vận hành) được gán cho bất kỳ người nào có quyền truy cập vào hệ thống được bảo mật. Quyền truy cập của người dùng được gắn với nhiệm vụ công việc của họ và bị giới hạn nên họ chỉ có đủ quyền truy cập để thực hiện các tác vụ cần thiết cho vị trí công việc của họ (nguyên tắc đặc quyền tối thiểu). Người dùng chịu trách nhiệm hiểu và duy trì chính sách bảo mật của một tổ chức bằng cách làm theo các quy trình hoạt động được quy định và hoạt động trong các thông số bảo mật được xác định.
- *Kiểm toán* có trách nhiệm xem xét và xác minh rằng chính sách an toàn được triển khai đúng và các giải pháp bảo mật được thực hiện đầy đủ. Vai trò kiểm

toán có thể được chỉ định cho chuyên gia bảo mật hoặc người dùng được đào tạo. Người kiểm toán đưa ra các báo cáo về việc tuân thủ và tính hiệu quả cho quản lý cấp cao xem xét. Các vấn đề được phát hiện thông qua các báo cáo này được chuyển thành các chỉ thị mới được chỉ định bởi người quản lý cấp cao cho các chuyên gia bảo mật hoặc người quản lý dữ liệu.

## 2.5 Phân loại thông tin và hệ thống thông tin

Việc phân loại cho các dạng dữ liệu khác nhau cho phép cơ quan/tổ chức công ty đánh giá chi phí và tài nguyên cần để bảo vệ từng loại dữ liệu bởi vì không phải tất cả dữ liệu đều có cùng giá trị với mỗi cơ quan/tổ chức. Có rất nhiều thông tin được tạo ra và duy trì trong quá trình hoạt động. Lý do để phân loại dữ liệu là sắp xếp dữ liệu theo độ nhạy cảm của nó đối với sự mất mát, tiết lộ hoặc không có sẵn. Khi dữ liệu được phân loại theo mức độ nhạy cảm của nó, người ta có thể quyết định những biện pháp kiểm soát an toàn nào là cần thiết để bảo vệ các loại dữ liệu khác nhau. Điều này đảm bảo rằng các tài sản thông tin nhận được mức bảo vệ thích hợp và các phân loại cho biết mức độ ưu tiên của bảo vệ an toàn đó. Mục đích chính của phân loại dữ liệu là cho biết mức độ bảo mật, tính toàn vẹn và tính sẵn sàng bảo vệ cần thiết cho từng loại tập dữ liệu.

Phân loại dữ liệu giúp đảm bảo dữ liệu được bảo vệ theo cách hiệu quả nhất về chi phí. Bảo vệ và duy trì dữ liệu tiêu tốn tiền của nhưng điều quan trọng là phải chi tiêu số tiền này cho thông tin thực sự cần bảo vệ. Mỗi loại cần có các yêu cầu xử lý riêng biệt và các thủ tục liên quan đến cách dữ liệu đó được truy cập, sử dụng và hủy. Ví dụ trong công ty, thông tin bí mật có thể được truy cập chỉ bởi quản lý cấp cao và một vài người trong toàn công ty. Để xóa dữ liệu này một cách chính xác khỏi phương tiện lưu trữ có thể cần phải thực hiện các quy trình khử bằng xung điện hoặc xóa zero.

Việc phân loại hệ thống thông tin cũng có yêu cầu tương tự như phân loại thông tin nhằm giúp cho cơ quan/tổ chức hiểu được mức độ quan trọng và triển khai các biện pháp bảo vệ phù hợp với hệ thống thông tin đang sở hữu.

Các thức phân loại thông tin và hệ thống thông tin tùy thuộc vào các áp dụng cơ quan/tổ chức. Tuy nhiên các tiêu chí khái quát nhất có thể gồm:

- Mức độ hữu ích
- Giá trị/chi phí
- Liên kết với cá nhân nào
- Đánh giá tổn thất khi lộ hay bị sửa đổi thông tin hay hệ thống bị xâm nhập
- Yêu cầu của quốc gia
- Các truy nhập được phép
- Các ràng buộc/hạn chế với thông tin và hệ thống

Có một số mô hình tiêu chuẩn hỗ trợ việc phân loại dữ liệu dựa trên các mô hình chính tắc như Bell-La Padula, Biba, Clark-Wilson. Mô hình Bell-La Padula được áp

dụng rộng rãi trong cơ quan chính quyền và quân sự của Hoa Kỳ với các lớp theo mức độ giảm dần bao gồm: tối mật (*top secret*), bí mật (*secret*), bảo mật (*confidential*), nhạy cảm nhưng chưa phân loại (s*ensitive but unclassified*), chưa được phân loại (u*nclassified*).

Chính phủ Việt Nam ban hành Nghị định số 85/2016/NĐ-CP về bảo đảm an toàn hệ thống thông tin theo cấp độ trong đó thông tin được phân loại thành 4 mức gồm có thông tin công cộng, thông tin riêng, thông tin cá nhân và thông tin bí mật nhà nước. Các hệ thống thông tin được phân loại theo nghiệp vụ bao gồm hệ thống nội bộ, hệ thống phục vụ người dân và cơ quan/tổ chức, hệ thống cơ sở hạ tầng,… Nghị định này cũng cung cấp các tiêu chí để xác định các 5 cấp độ khác nhau của hệ thống thông tin.

## 2.6 Mô hình mối đe dọa

### 2.6.1 *Giới thiệu*

Mô hình hóa mối đe dọa là quá trình bảo mật trong đó các mối đe dọa tiềm ẩn được xác định, phân loại và phân tích. Mô hình hóa mối đe dọa có thể được thực hiện như một biện pháp chủ động trong quá trình thiết kế và phát triển hoặc như một biện pháp đối phó sau khi sản phẩm đã được triển khai. Trong cả hai trường hợp, quy trình xác định tác hại tiềm ẩn, xác suất xảy ra, mức độ ưu tiên cần quan tâm và các phương tiện để loại bỏ hoặc giảm thiểu mối đe dọa.

Mô hình mối đe dọa không có nghĩa là một sự kiện duy nhất. Thay vào đó, cơ quan/ tổ chức thường bắt đầu lập mô hình mối đe dọa sớm trong quá trình thiết kế hệ thống và tiếp tục trong suốt vòng đời của nó nhằm hai mục tiêu:

- Để giảm số lượng các lỗi thiết kế và mã hóa liên quan đến bảo mật
- Để giảm mức độ nghiêm trọng của bất kỳ khuyết tật còn lại nào

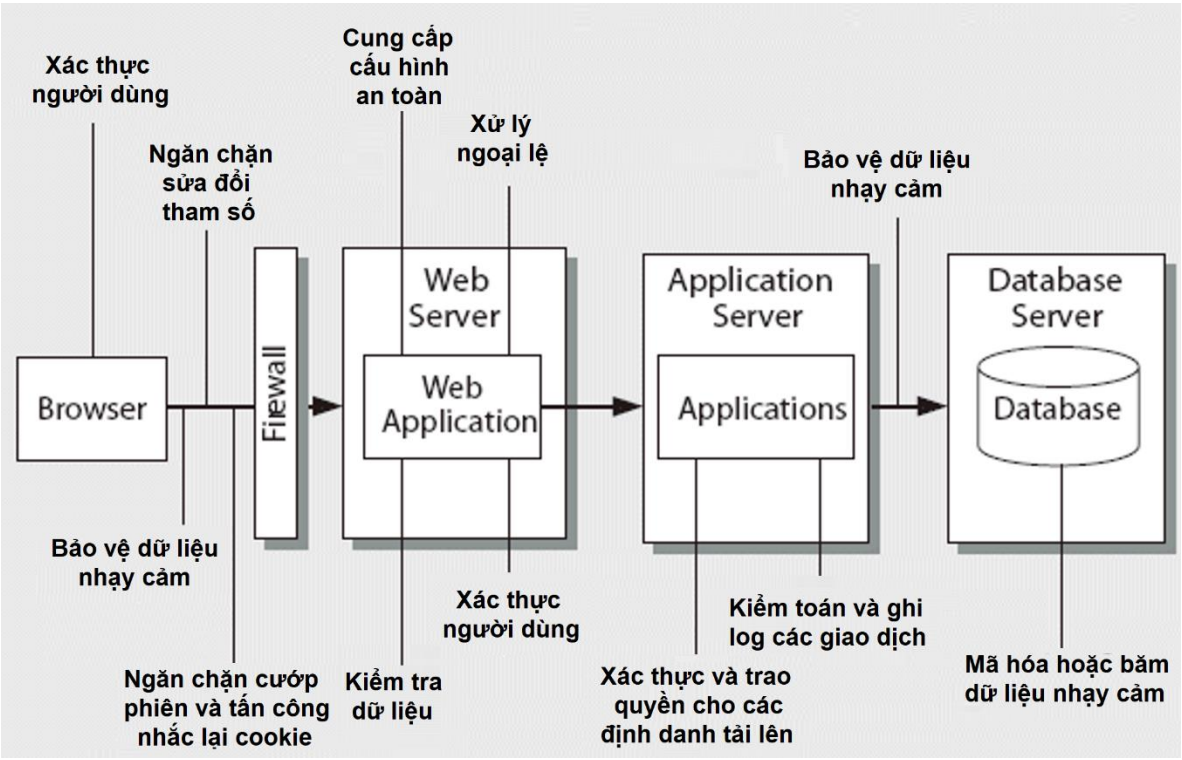
Nói cách khác, cách tiếp cận này cố gắng giảm thiểu các lỗ hổng và giảm tác động của bất kỳ lỗ hổng nào còn sót lại. Một cách tiếp cận chủ động thực hiện mô hình hóa mối đe dọa diễn ra trong giai đoạn đầu của quá trình phát triển hệ thống, đặc biệt là trong quá trình thiết lập thông số kỹ thuật và thiết kế ban đầu. Phương pháp này dựa trên việc dự đoán các mối đe dọa và thiết kế các biện pháp phòng thủ cụ thể trong quá trình mã hóa và chế tạo, thay vì dựa vào các bản vá và cập nhật sau triển khai. Trong hầu hết các trường hợp, các giải pháp bảo mật tích hợp hiệu quả hơn về chi phí và thành công hơn những giải pháp được cải tiến sau này. Tuy vậy, không phải tất cả các mối đe dọa đều có thể được dự đoán trong giai đoạn thiết kế, do đó, mô hình mối đe dọa theo cách tiếp cận đối phó vẫn cần thiết để giải quyết các vấn đề không lường trước được.

Cách tiếp cận đối phó mô hình hóa mối đe dọa diễn ra sau khi sản phẩm đã được tạo và triển khai. Việc triển khai này có thể trong môi trường thử nghiệm hoặc phòng thí nghiệm hoặc trên thị trường chung. Kỹ thuật mô hình hóa mối đe dọa này là khái niệm cốt lõi đằng sau bẻ khóa một cách đạo đức, kiểm tra thâm nhập, xem xét mã nguồn và kiểm tra dữ liệu (*fuzzing*). Mặc dù các quy trình này thường hữu ích trong việc tìm ra các

lỗ hổng và các mối đe dọa cần được giải quyết, nhưng rất tiếc, chúng dẫn đến bổ sung đoạn mã để thực hiện các biện pháp đối phó mới. Quay trở lại giai đoạn thiết kế có thể tạo ra các sản phẩm tốt hơn về lâu dài, nhưng việc bắt đầu lại từ đầu sẽ rất tốn kém và gây ra sự chậm trễ đáng kể về thời gian cho việc phát hành sản phẩm. Do đó, cách tiết kiệm là tạo các bản cập nhật hoặc bản vá để thêm vào sản phẩm sau khi triển khai. Điều này lại dẫn đến các cải tiến bảo mật kém hiệu quả hơn với phí tổn về chức năng và tính thân thiện với người dùng.

### 2.6.2 *Các vấn đề kiến trúc và thiết kế ứng dụng Web*

Các ứng dụng web đặt ra cho các nhà thiết kế và nhà phát triển nhiều thách thức. Bản chất không trạng thái của HTTP có nghĩa là việc theo dõi trạng thái phiên của mỗi người dùng trở thành trách nhiệm của ứng dụng. Trước đây, ứng dụng phải có khả năng xác định người dùng bằng cách sử dụng một số hình thức xác thực. Với việc cho rằng tất cả các quyết định ủy quyền tiếp theo đều dựa trên danh tính của người dùng, điều quan trọng là quy trình xác thực phải an toàn và cơ chế xử lý phiên được sử dụng để theo dõi người dùng đã xác thực cũng được bảo vệ tốt như nhau. Thiết kế xác thực an toàn và cơ chế quản lý phiên chỉ là một vài vấn đề mà các nhà thiết kế và phát triển ứng dụng Web phải đối mặt. Những thách thức khác xảy ra vì dữ liệu đầu vào và đầu ra đi qua các mạng công cộng. Ngăn chặn sửa đổi tham số và tiết lộ dữ liệu nhạy cảm là những vấn đề hàng đầu khác.




**Hình 2-1. Các vấn đề an toàn tại các lớp ứng dụng Web**

Một số vấn đề hàng đầu cần giải quyết bằng các thực tiễn thiết kế an toàn được thể hiện trong dưới đây dựa theo khuyến nghị của Microsoft. Hình vẽ trên thể hiện kiến trúc

đa lớp tiêu biểu cho ứng dụng Web bắt đầu từ trình duyệt người dùng, tới máy chủ Web, máy chủ ứng dụng và máy chủ cơ sở dữ liệu. Các lớp trong mô hình tham chiếu này là tiêu biểu cho các chức năng căn bản của ứng dụng Web.

Các lỗ hổng và vấn đề tiềm tàng do thiết kế không tốt cũng như cách tiếp cận được trình bày như dưới đây.

- *Đầu vào / Xác thực dữ liệu*: Vấn đề phát sinh do chèn các chuỗi độc hại trong các phần tử giao diện người dùng hoặc các API công khai. Các cuộc tấn công này bao gồm thực thi lệnh, viết mã trang web chéo (XSS), chèn SQL và tràn bộ đệm. Hậu quả có thể bao gồm từ tiết lộ thông tin đến nâng cao đặc quyền và thực thi mã tùy ý.

  Xác thực đầu vào là một vấn đề đầy thách thức và gánh nặng chính với giải pháp của các nhà phát triển ứng dụng. Tuy nhiên, xác thực đầu vào thích đáng là một trong những biện pháp bảo vệ hưu hiệu nhất trước các cuộc tấn công ứng dụng ngày nay. Xác thực đầu vào thích hợp là một biện pháp đối phó hiệu quả có thể giúp ngăn chặn XSS, SQL injection, tràn bộ đệm và các cuộc tấn công đầu vào khác.

  Xác thực đầu vào là một thách thức vì không có câu trả lời duy nhất cho những gì cấu thành đầu vào hợp lệ trên các ứng dụng hoặc thậm chí trong các ứng dụng. Tương tự như vậy, không có định nghĩa duy nhất về đầu vào độc hại. Thêm vào khó khăn này là những gì ứng dụng làm với đầu vào ảnh hưởng đến việc nguy cơ bị khai thác. Ví dụ: dữ liệu được lưu trữ để sử dụng bởi các ứng dụng khác hay ứng dụng sử dụng dữ liệu đầu vào từ các nguồn dữ liệu được tạo bởi các ứng dụng khác. Các nguyên tắc cơ bản sau đây cải thiện xác thực đầu vào của ứng dụng Web của bạn:

  - Coi tất cả các đầu vào là độc hại,
  - Sử dụng cách tiếp cận tập trung hóa,
  - Không dựa vào xác thực phía máy khách,
  - Hãy cẩn thận với các vấn đề về chuẩn hóa,
  - Ràng buộc, từ chối và thanh lọc đầu vào.

- *Xác thực*: Bị tấn công qua giả mạo danh tính, bẻ khóa mật khẩu, nâng cao đặc quyền và truy cập trái phép. Xác thực là quá trình xác định danh tính người gọi. Có ba khía cạnh cần xem xét:

  - Xác định nơi cần xác thực trong ứng dụng. Nó thường được yêu cầu bất cứ khi nào vượt qua ranh giới tin cậy thường bao gồm các quy trình và máy tính.
  - Xác thực người gọi là ai. Người dùng thường tự xác thực bằng tên người dùng và mật khẩu.
  - Xác định người dùng trong các yêu cầu tiếp theo. Điều này yêu cầu một số hình thức mã thông báo xác thực.

Nhiều ứng dụng Web sử dụng cơ chế mật khẩu để xác thực người dùng, trong đó người dùng cung cấp tên người dùng và mật khẩu dưới dạng HTML. Các biện pháp sau đây cải thiện xác thực ứng dụng Web của bạn:

- Tách biệt khu vực công cộng và khu vực hạn chế,
- Sử dụng chính sách khóa tài khoản cho tài khoản người dùng cuối,
- Hỗ trợ thời gian hết hạn mật khẩu,
- Có thể vô hiệu hóa tài khoản,
- Không lưu trữ mật khẩu trong ở phía người dùng,
- Yêu cầu mật khẩu mạnh,
- Không gửi mật khẩu ở dạng văn bản rõ ràng,
- Bảo vệ cookie xác thực.

- *Ủy quyền*: Bị truy cập vào dữ liệu bí mật hoặc bị hạn chế, giả mạo dữ liệu và thực hiện các hoạt động trái phép.

  Ủy quyền xác định những gì danh tính được xác thực có thể làm và các tài nguyên có thể được truy cập. Việc ủy quyền không đúng cách hoặc yếu kém dẫn đến tiết lộ thông tin và giả mạo dữ liệu. Bảo vệ theo chiều sâu là nguyên tắc bảo mật quan trọng để áp dụng cho chiến lược ủy quyền ứng dụng. Các phương pháp sau đây cải thiện việc ủy quyền ứng dụng Web:
  - Sử dụng nhiều cổng kiểm tra,
  - Hạn chế quyền truy cập của người dùng vào tài nguyên cấp hệ thống,
  - Xem xét mức độ chi tiết của ủy quyền.
- *Quản lý cấu hình*: Bị truy cập trái phép vào các giao diện quản trị, khả năng cập nhật dữ liệu cấu hình và truy cập trái phép vào tài khoản người dùng và hồ sơ tài khoản.

  Xem xét cẩn thận chức năng quản lý cấu hình ứng dụng Web. Hầu hết các ứng dụng yêu cầu giao diện cho phép nhà phát triển nội dung, nhà điều hành và quản trị viên cấu hình ứng dụng và quản lý các mục như nội dung trang Web, tài khoản người dùng, thông tin hồ sơ người dùng và chuỗi kết nối cơ sở dữ liệu. Nếu quản trị từ xa được hỗ trợ, các giao diện quản trị được bảo mật một cách thích đáng. Hậu quả của vi phạm bảo mật đối với giao diện quản trị có thể rất nghiêm trọng, vì kẻ tấn công thường chạy với các đặc quyền của quản trị viên và có quyền truy cập trực tiếp vào toàn bộ trang web. Các phương pháp sau đây cải thiện tính bảo mật của việc quản lý cấu hình ứng dụng Web:
  - Bảo mật các giao diện quản trị,
  - Bảo mật kho lưu trữ cấu hình,
  - Duy trì các đặc quyền quản trị riêng biệt,
  - Sử dụng các tài khoản dịch vụ và quy trình ít đặc quyền nhất.
- *Dữ liệu nhạy cảm*: Bị tiết lộ thông tin bí mật và giả mạo dữ liệu.

Các ứng dụng xử lý thông tin riêng tư của người dùng như số thẻ tín dụng, địa chỉ, hồ sơ y tế, v.v. phải thực hiện các bước đặc biệt để đảm bảo rằng dữ liệu vẫn riêng tư và không bị thay đổi. Ngoài ra, các bí mật được sử dụng bởi việc triển khai ứng dụng, chẳng hạn như mật khẩu và chuỗi kết nối cơ sở dữ liệu, phải được bảo mật. Bảo mật của dữ liệu nhạy cảm là một vấn đề trong khi dữ liệu được lưu trữ trong bộ nhớ ổn định và trong khi nó được truyền qua mạng.
Bí mật bao gồm mật khẩu, chuỗi kết nối cơ sở dữ liệu và số thẻ tín dụng. Các phương pháp sau đây cải thiện tính bảo mật của việc xử lý các bí mật trong ứng dụng Web:

- Không cất giữ bí mật nếu có thể tránh,
- Không lưu trữ bí mật trong đoạn mã,
- Không lưu trữ các kết nối cơ sở dữ liệu, mật khẩu hoặc khóa trong văn bản rõ ràng,
- Tránh lưu trữ bí mật trong Cơ quan an ninh địa phương,
- Sử dụng API bảo vệ dữ liệu để mã hóa bí mật.

- *Mã hóa*: Bị truy cập vào dữ liệu bí mật hoặc thông tin đăng nhập tài khoản hoặc cả hai.
  Các ứng dụng web thường sử dụng mã hóa để bảo mật dữ liệu trong các kho lưu trữ ổn định hoặc khi nó được truyền qua các mạng. Các phương pháp sau đây cải thiện tính bảo mật của ứng dụng Web khi sử dụng mật mã:
  - Không phát triển cách mã hóa của riêng,
  - Giữ dữ liệu chưa được mã hóa gần với thuật toán,
  - Sử dụng đúng thuật toán và kích thước khóa chính xác,
  - Bảo mật các khóa mã hóa.
- *Quản lý ngoại lệ*: Bị từ chối dịch vụ và tiết lộ các chi tiết nhạy cảm ở cấp hệ thống.
  Xử lý ngoại lệ an toàn có thể giúp ngăn chặn một số cuộc tấn công từ chối dịch vụ ở cấp ứng dụng và nó cũng có thể được sử dụng để ngăn thông tin cấp hệ thống có giá trị hữu ích cho những kẻ tấn công được trả lại cho máy khách.
  Ví dụ: nếu không có xử lý ngoại lệ thích hợp, thông tin như chi tiết lược đồ cơ sở dữ liệu, phiên bản hệ điều hành, dấu vết ngăn xếp, tên tệp và thông tin đường dẫn, chuỗi truy vấn SQL và thông tin khác có giá trị cho kẻ tấn công có thể được trả lại cho máy khách.
  Một cách tiếp cận tốt là thiết kế một giải pháp quản lý ngoại lệ và ghi log tập trung và xem xét cung cấp các móc nối vào hệ thống quản lý ngoại lệ để hỗ trợ thiết bị đo đạc và giám sát tập trung để giúp quản trị viên hệ thống. Các phương pháp sau đây giúp bảo mật quản lý ngoại lệ của ứng dụng Web của bạn:
  - Không để rò rỉ thông tin cho khách hàng,
  - Ghi thông báo lỗi chi tiết,

- Xử lý các trường hợp ngoại lệ.

- *Kiểm toán và Ghi log*: Không phát hiện được dấu hiệu xâm nhập, không có khả năng chứng minh hành động của người dùng và khó khăn trong việc chẩn đoán sự cố.

  Nên kiểm tra và ghi lại hoạt động trên các cấp ứng dụng. Sử dụng log có thể phát hiện hoạt động đáng ngờ. Điều này thường cung cấp các dấu hiệu ban đầu về một cuộc tấn công toàn diện và các bản ghi giúp giải quyết mối đe dọa từ chối khi người dùng từ chối hành động của họ. Hồ sơ log có thể được yêu cầu trong thủ tục pháp lý để chứng minh hành vi sai trái của các cá nhân. Nói chung, đánh giá được coi là có thẩm quyền nhất nếu các cuộc đánh giá được thực hiện vào thời điểm chính xác của việc truy cập tài nguyên và theo cùng một thủ tục truy cập tài nguyên. Các biện pháp sau đây cải thiện tính bảo mật:
  - Kiểm tra và đăng nhập quyền truy cập trên các cấp ứng dụng.
  - Xem xét luồng danh tính.
  - Ghi log các sự kiện chính.
  - Bảo mật các file log.
  - Sao lưu và phân tích các log thường xuyên.

Vấn đề an toàn phải xuyên suốt mọi giai đoạn của vòng đời phát triển sản phẩm và nó phải là trọng tâm của thiết kế ứng dụng Web. Đặc biệt cần thiết thiết kế một chiến lược xác thực và ủy quyền vững chắc. Phần lớn các cuộc tấn công ở cấp độ ứng dụng dựa trên dữ liệu đầu vào được hình thành độc hại và xác thực đầu vào ứng dụng kém. Các vấn đề và cách tiếp cận ở đây sẽ người đọc hình dung các khía cạnh rủi ro và thách thức đảm bảo an toàn trong phân tích và đánh giá các ứng dụng an toàn.

## 2.7 Câu hỏi ôn tập

1. Khái niệm về kế hoạch an toàn của cơ quan/tổ chức.
2. Các bước cơ bản trong việc xây dựng kế hoạch an toàn.
3. Trình bày nguyên tắc phân loại thông tin và hệ thống thông tin.
4. Nêu và diễn giải các nhiệm vụ cơ bản của quản lý an toàn thông tin?
5. Trình bày cách thức tổ chức quản lý an toàn thông tin?
6. Tại sao cần phân loại thông tin và hệ thống thông tin.
7. Tại sao cần có mô hình đe dọa?
8. Nêu các lỗ hổng tiêu biểu trong việc thiết kế và xây dựng ứng dụng Web?
9. Nêu các vấn đề về an toàn trong việc thiết kế ứng dựng thương mại điện tử?
10. Nêu các mối đe dọa về an toàn cơ bản khi xây dựng ứng dụng truy vết tiếp xúc?

# CHƯƠNG 3. HỆ THỐNG QUẢN LÝ AN TOÀN THÔNG TIN

Chương này tập trung trình bày cách thức phân tích và đánh giá rủi ro của các biện pháp kiểm soát với các vấn đề về an toàn hay các lỗ hổng giúp cho người quản lý có thể ra quyết định phù hợp cũng như xác định mức độ rủi ro chấp nhận được. Cách thức triển khai và đặc trưng của các tiêu chuẩn thực tế cho việc phân tích rủi ro bao gồm OCTAVE, NIST SP 800-30 và ISO 27005 được giới thiệu chi tiết trong phần này.

## 3.1 Quản lý an toàn

Quản lý an toàn thay đổi hàng năm do các máy tính, môi trường mạng và các ứng dụng xử lý thông tin thay đổi. Máy tính cá nhân ngày trở nên mạnh hơn, môi trường mạng kết nối càng rộng rãi hơn, người dùng có nhiều thông tin về hoạt động của hệ thống máy tính hơn, thông tin phân tán ra khắp các thiết bị khác nhau trong mạng. Việc này khiến cho vấn đề quản lý an toàn thông tin phức tạp và nghiêm trọng hơn. Mặt khác, thông tin và dữ liệu trở nên quan trọng hơn cả tài sản vật lý khác như thiết bị hay nhà xưởng.

Quản lý an toàn bao gồm tất cả các hoạt động cần thiết để giữ cho một chương trình an toàn hoạt động và phát triển. Việc này bao gồm quản lý rủi ro, lập tài liệu, quản lý và triển khai các biện pháp kiểm soát an toàn, quy trình và thủ tục, an toàn nhân sự, kiểm toán và đào tạo nâng cao nhận thức an toàn liên tục.

Việc phân tích rủi ro xác định các tài sản quan trọng, phát hiện ra các mối đe dọa, xếp chúng vào nguy cơ và được sử dụng để ước tính thiệt hại có thể và tổn thất tiềm ẩn mà cơ quan/tổ chức có thể chịu đựng. Phân tích rủi ro giúp quản lý xây dựng ngân sách với các quỹ cần thiết để bảo vệ tài sản được ghi nhận khỏi các mối đe dọa được xác định và phát triển các chính sách an toàn giúp định hướng cho các hoạt động an ninh. Các biện pháp bảo vệ được xác định, triển khai và duy trì để giữ rủi ro bảo mật của tổ chức ở mức có thể chấp nhận được. Việc giáo dục an ninh và nhận thức đưa thông tin này đến từng nhân viên trong cơ quan/tổ chức để mọi người được thông tin đầy đủ và có thể dễ dàng làm việc hơn hướng tới cùng mục tiêu an toàn.

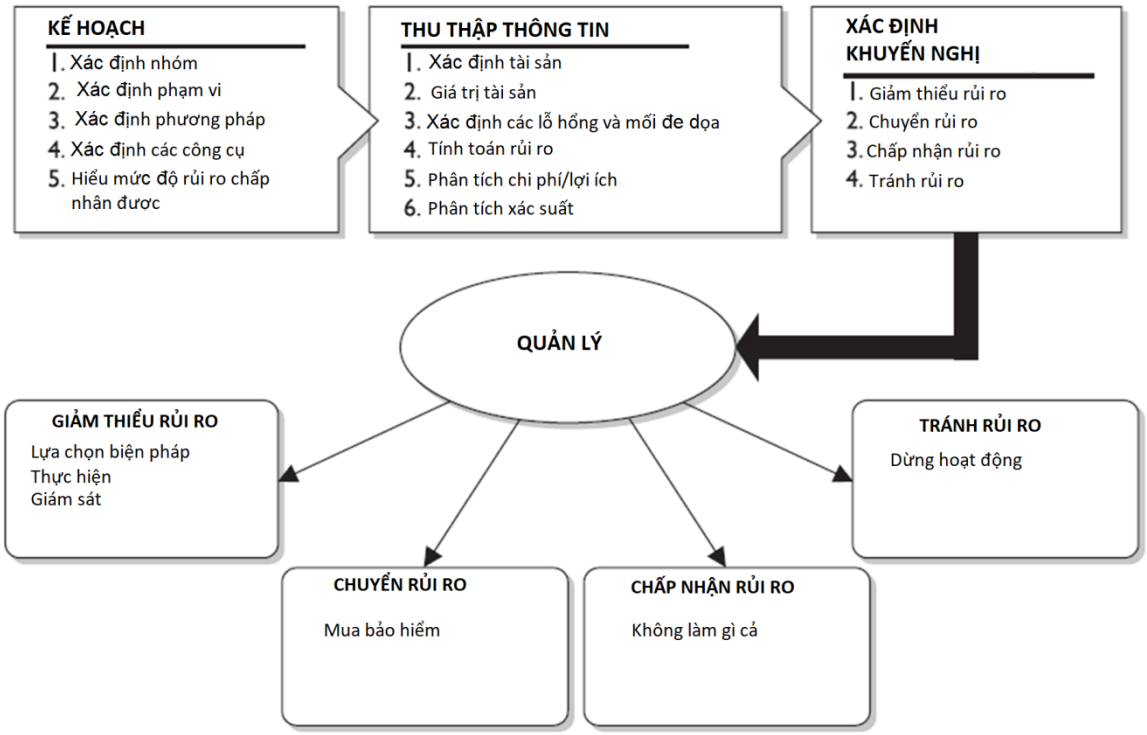
ISMS và kiến trúc an toàn doanh nghiệp có sự khác biệt. ISMS phác thảo các biện pháp kiểm soát cần thực thi (quản lý rủi ro, quản lý lỗ hổng, kế hoạch duy trì hoạt động, bảo vệ dữ liệu, kiểm tra, quản lý cấu hình, bảo mật vật lý v.v.) và cung cấp hướng dẫn về các biện pháp này trong suốt vòng đời của chúng. ISMS quy định cụ thể các phần và bộ phận cần được đưa vào để đưa ra chương trình an toàn toàn diện cho cơ quan/tổ chức nói chung và cách duy trì đúng cách các phần và bộ phận đó. Kiến trúc an toàn doanh nghiệp cho biết cách các thành phần này được tích hợp vào các lớp khác nhau của môi trường hoạt động hiện tại. Các thành phần an toàn của ISMS phải được đan xen trong môi

trường hoạt động và không bị giới hạn trong các phòng ban riêng biệt. Ví dụ, ISMS chỉ định việc quản lý rủi ro cần được thực hiện và kiến trúc doanh nghiệp cho biết cách quản lý rủi ro diễn ra ở cấp độ chiến lược, chiến thuật và hoạt động.

Bộ tiêu chuẩn ISO/ IEC 27000 (nêu ra ISMS) hướng chính sách và phác thảo các thành phần cần thiết của một chương trình an toàn. Điều này có nghĩa là các tiêu chuẩn ISO có tính chất tổng quát và được tạo ra theo cách để chúng có thể được áp dụng cho nhiều loại hình doanh nghiệp, công ty và tổ chức khác nhau. Nhưng vì các tiêu chuẩn này là chung, rất khó để biết cách triển khai chúng và ánh xạ chúng tới cơ sở hạ tầng và nhu cầu hoạt động hay kinh doanh của cơ quan/tổ chức cụ thể. Đây là nơi mà kiến trúc an toàn phát huy tác dụng. Kiến trúc là một công cụ được sử dụng để đảm bảo rằng những gì được nêu trong các tiêu chuẩn bảo mật được thực hiện xuyên suốt các lớp khác nhau của cơ quan/tổ chức.

## 3.2 Quản lý rủi ro

Trong ngữ cảnh an toàn các hư hỏng có thể xảy ra và cần phân nhánh những tổn hại đó. Việc quản lý rủi ro thông tin là quá trình nhận dạng và đánh giá các rủi ro, giảm thiểu chúng đến mức chấp nhận được và triển khai các cơ chế phù hợp để duy trì mức độ đó. Hình dưới đây mô tả các thành phần cơ bản của việc quản lý rủi ro.




**Hình 3-1. Các bước quản lý rủi ro**

Không có môi trường nào an toàn một cách hoàn hảo, rủi ro có thể xuất hiện ở nhiều dạng khác nhau. Một số dạng rủi ro cơ bản

- Vật lý: cháy, ngập, thảm họa tự nhiên
- Con người: Hành động bất ngờ hay có chủ ý làm gián đoạn hoạt động sản xuất
- Hỏng thiết bị: Hư hỏng hệ thống hay các thiết bị ngoại vi
- Tấn công từ bên trong và bên ngoài: Bẻ khóa, tấn công
- Lạm dụng dữ liệu: Lừa đảo, chia sẻ bí mật thương mại, gián điệp
- Mất dữ liệu: Mất có hay không có chủ ý do sử dụng không được phép
- Lỗi chương trình: Lỗi tính toán, đầu vào, tràn bộ đệm

Các mối đe dọa phải được xác định, phân loại theo danh mục và được đánh giá để tính toán khả năng thiệt hại của chúng đối với cơ quan/tổ chức. Nguy cơ thực sự khó đo lường nhưng ưu tiên các rủi ro tiềm ẩn theo thứ tự mà những rủi ro phải được giải quyết trước tiên là điều có thể thực hiện được.

An toàn là một vấn đề với hoạt động hay kinh doanh nhưng các cơ quan/tổ chức hoạt động để phát triển chứ không chỉ để được an toàn. Cơ quan/tổ chức chỉ quan tâm đến vấn đề an toàn nếu rủi ro tiềm ẩn đe dọa nghiêm trọng tới cơ quan/tổ chức chẳng hạn như qua mất danh tiếng hay cơ sở dữ liệu khách hàng bị xâm nhập

Thực hiện quản lý rủi ro đúng cách mang lại hiểu biết toàn diện về tổ chức của mình gồm có các mối đe dọa mà nó phải đối mặt, các biện pháp đối phó có thể được đưa ra để xử lý với các mối đe dọa đó và giám sát liên tục để đảm bảo mức độ chấp nhận được.

Nhóm quản lý rủi ro có quy mô phù hợp với kích cỡ của cơ quan/tổ chức, quy mô nguồn lực để đạt được mục tiêu bảo đảm yêu cầu an toàn thông tin với cách thức hiệu quả nhất. Nhóm quản lý rủi ro cần xác định được các mục tiêu căn bản sau:

- Mức rủi ro chấp nhận được mà được xác lập bởi quản lý cấp cao
- Thủ tục và quy trình đánh giá rủi ro
- Thủ tục xác định và giảm thiểu rủi ro
- Nguồn lực phù hợp và phân bổ tài chính từ quản lý cấp cao
- Đào tạo nhận thức an ninh cho toàn bộ cán bộ/nhân viên cùng với tài sản thông tin
- Khả năng thiết lập nhóm ứng phó theo lĩnh vực cụ thể khi cần thiết. Chỉ rõ các yêu cầu tuân thủ các quy định và luật pháp để kiểm soát và thực hiện các yêu cầu này.
- Phát triển các số đo và chỉ số hiệu năng để đo lường và quản lý các loại rủi ro khác nhau
- Khả năng xác định và đánh giá rủi ro mới khi thay đổi môi trường làm việc của công ty.
- Tích hợp với quy trình kiểm soát thay đổi của cơ quan để chắc chắn rằng việc thay đổi không đưa ra các lỗ hổng mới

## 3.3 Nhận dạng, phân tích và đánh giá rủi ro

### 3.3.1 *Khái niệm*

*Nhận dạng* là quá trình xác định các tài sản có giá trị với cơ quan/tổ chức có nguy cơ bị tác động bởi lỗ hổng hay mối đe doạ tiềm tàng. *Đánh giá rủi ro* là phương pháp nhận biết lỗ hổng, mối đe dọa và đánh giá tác động có thể để xác định vị trí triển khai các biện pháp kiểm soát. Đánh giá rủi ro thực sự là một công cụ để quản lý rủi ro và phân tích hậu quả của các rủi ro. *Phân tích rủi ro* đảm bảo an toàn có chi phí hiệu quả, thích đáng, kịp thời và sẵn sàng phản ứng lại với các đe dọa. An toàn có thể khá phức tạp ngay cả đối với các chuyên gia bảo mật thông thạo. Mặt khác, rất dễ áp dụng an toàn quá mức cũng như không đủ an toàn hoặc biện pháp kiểm soát sai hay chi tiêu quá nhiều tiền trong quá trình mà không đạt được các mục tiêu cần thiết.

*Phân tích rủi ro* giúp các cơ quan/tổ chức phân loại rủi ro và chứng tỏ việc quản lý khối lượng tài nguyên bao gồm nhân lực và tài lực cần được áp dụng để bảo vệ chống lại những rủi ro đó một cách hợp lý. Phân tích rủi ro hướng đến các mục tiêu căn bản:

- Xác định tài sản và giá trị của chúng
- Xác định lỗ hổng và các mối đe dọa
- Định lượng xác suất và ảnh hưởng tới công việc của các mối đe dọa tiềm năng
- Xác định cân bằng kinh tế giữa tác động của mối đe dọa và chi phí của biện pháp phòng chống.

Một trong những nhiệm vụ của phân tích rủi ro là báo cáo chi tiết việc xác định giá trị tài sản. Quản lý cấp cao cần xem xét và phê duyệt danh sách và đưa các tài sản vào phân tích đánh giá rủi ro. Trong giai đoạn đầu, nếu một số tài sản được cho là không quan trọng thì nhóm đánh giá rủi ro không nên dành thêm thời gian hoặc tài nguyên để đánh giá các tài sản đó. Việc đánh giá căn cứ vào các thuộc tính an toàn: tính sẵn dùng và tính toàn vẹn và bảo mật, và chúng liên quan trực tiếp đến nhu cầu hoạt động như thế nào.

Phân tích rủi ro giúp tích hợp mục tiêu chương trình an toàn với các mục tiêu và yêu cầu hoạt động của cơ quan/tổ chức. Càng có nhiều gắn kết giữa mục tiêu hoạt động và an toàn thì sẽ thành công hơn với cả hai mục tiêu. Việc phân tích cũng giúp dự thảo ngân sách phù hợp cho chương trình bảo mật và các thành phần cấu thành của nó. Khi một cơ quan/tổ chức biết được giá trị tài sản của mình và các mối đe dọa có thể xảy ra, họ có thể đưa ra các quyết định hợp lý về chi phí cho việc bảo vệ những tài sản đó.

Phân tích rủi ro phải được hỗ trợ và chỉ đạo bởi quản lý cấp cao để thành công. Việc quản lý phải xác định mục đích và phạm vi phân tích, chỉ định một nhóm thực hiện đánh giá. Bên cạnh đó, cần phân bổ thời gian và kinh phí cần thiết để tiến hành phân tích. Điều cần thiết cho quản lý cấp cao là xem xét kết quả của việc đánh giá và phân tích rủi ro và xử lý các kết quả của việc phân tích.

### 3.3.2 *Xác định giá trị thông tin và tài sản*

Giá trị của thông tin có tính chất tương đối phụ thuộc vào các yếu tố:

- Các bên liên quan,
- Công sức cần thiết để phát triển,
- Chi phí duy trì,
- Tổn thất hay hư hỏng khi bị mất hay phá hủy,
- Đối thủ muốn trả bao nhiêu để có được thông tin đó,
- Ràng buộc trách nhiệm pháp lý.

Nếu cơ quan không biết giá trị của thông tin và các tài sản khác mà cơ quan đó đang nỗ lực bảo vệ, thì họ không biết phải tốn bao nhiêu tiền và thời gian để bảo vệ chúng. Giá trị của thông tin củng cố các quyết định về biện pháp an ninh. Giá trị của các cơ sở và phương tiện của cơ quan cũng phải được đánh giá cùng với tất cả các thiết bị như máy in, máy trạm, máy chủ, thiết bị ngoại vi, nguồn cung cấp và nhân viên.

Tài sản có thể được xác định bằng cách định tính hay định lượng. Các biện pháp này phải được đưa ra một cách rõ ràng. Giá trị thực tế của tài sản được quyết định bởi mức độ quan trọng của tài sản đối với cơ quan/tổ chức. Các yếu tố sau ảnh hưởng đến giá trị của tài sản:

- Chi phí sở hữu hay phát triển tài sản
- Chi phí duy trì và bảo vệ tài sản
- Giá trị đối với chủ sở hữu và người dùng
- Giá trị đối với đối thủ
- Mức giá mà người ta trả cho tài sản đó
- Chi phí thay thế khi mất
- Các hoạt động điều hành và sản xuất bị ảnh hưởng nếu không có sẵn tài sản đó
- Trách nhiệm pháp lý nếu tài sản đó bị thất thoát
- Tính hữu dụng và vai trò của tài sản trong cơ quan

Hiểu được giá trị của tài sản là bước đầu tiên để biết được những cơ chế an toàn nào nên được đặt ra và những nguồn lực nên hướng tới bảo vệ nó. Cũng như vậy, một câu hỏi rất quan trọng là mức tổn hại như thế nào khi cơ quan không thể bảo vệ tài sản của mình. Việc xác định giá trị tài sản có thể hữu ích vì nhiều lý do, bao gồm:

- Để thực hiện phân tích chi phí/lợi ích hiệu quả
- Để lựa chọn biện pháp đối phó và biện pháp bảo vệ cụ thể
- Để xác định mức độ bao trả bảo hiểm để mua
- Để hiểu chính xác những gì đang có nguy cơ
- Tuân thủ các yêu cầu pháp lý và quy định

Tài sản có thể hữu hình (máy tính, phương tiện, vật tư) hoặc vô hình (danh tiếng, dữ liệu, sở hữu trí tuệ). Thường khó xác định giá trị của tài sản vô hình và có thể thay đổi

theo thời gian. Không dễ để xác định danh tiếng đáng giá bao nhiêu song điều quan trọng là có thể thực hiện được việc này.

### 3.3.3 *Xác định đe dọa và lỗ hổng*

Rủi ro có thể coi là xác suất của một tác nhân đe dọa khai thác thành công một lỗ hổng để gây hại cho một tài sản và tác động lên kết quả hoạt động của cơ quan/tổ chức. Nhiều loại tác nhân đe dọa có thể tận dụng một số loại lỗ hổng và dẫn đến một loạt các mối đe dọa cụ thể như các trường hợp trong Bảng 3-1 dưới đây. Đây là các trường hợp tiêu biểu nhiều cơ quan/tổ chức cần giải quyết trong các chương trình quản lý rủi ro của họ.

Các loại mối đe dọa khác có thể phát sinh trong một môi trường khó xác định hơn những loại được nêu ví dụ. Những mối đe dọa khác sử dụng các lỗi ứng dụng và người dùng. Nếu ứng dụng phức tạp thì mối đe dọa có thể khó phát hiện và cô lập như sử dụng dữ liệu được nhập không chính xác. Điều này có thể dẫn đến việc xử lý không phù hợp và các lỗi lại được chuyển sang tiến trình khác. Những loại vấn đề này có thể nằm trong mã của ứng dụng và rất khó xác định.

**Bảng 3-1. Các tác nhân đe dọa và lỗ hổng.**

| **Tác nhân** | **Khai thác lỗ hổng** | **Hậu quả** |
|---|---|---|
| Phần mềm độc hại | Thiếu phần mềm chống vi-rút | Nhiễm vi-rút |
| Người bẻ khóa | Các dịch vụ quan trọng chạy trên máy chủ | Truy cập trái phép vào thông tin bí mật |
| Người dùng | Tham số được định cấu hình sai trong hệ điều hành | Sự cố hệ thống |
| Cháy | Thiếu bình chữa cháy | Thiệt hại cơ sở và máy tính, và có thể mất mạng |
| Nhân viên | Thiếu đào tạo hoặc thực thi tiêu chuẩn<br>Thiếu kiểm toán | Chia sẻ thông tin quan trọng về nhiệm vụ<br>Thay đổi dữ liệu đầu vào và đầu ra từ các ứng dụng xử lý dữ liệu |
| Kẻ tấn công | Ứng dụng được viết kém<br>Thiếu cài đặt tường lửa nghiêm ngặt | Thực hiện tấn công tràn bộ đệm<br>Thực hiện cuộc tấn công từ chối dịch vụ |
| Nhà thầu | Thiếu cơ chế kiểm soát truy cập | Ăn cắp bí mật thương mại |
| Kẻ xâm nhập | Thiếu bảo vệ an ninh | Phá cửa và ăn cắp máy tính và thiết bị |

Lỗi người dùng, cố tình hoặc vô tình, dễ xác định hơn bằng cách giám sát và kiểm tra hoạt động của người dùng. Việc kiểm tra và đánh giá phải được tiến hành để phát hiện xem nhân viên có nhập các giá trị không chính xác vào các chương trình, lạm dụng công nghệ hoặc sửa đổi dữ liệu một cách không phù hợp hay không.

Một khi các lỗ hổng và các mối đe dọa liên quan được xác định, các rẽ nhánh của các lỗ hổng này đang được khai thác phải được điều tra. Rủi ro hàm chứa tổn thất, có nghĩa là những thứ mất đi nếu tác nhân đe dọa thực sự khai thác thành công một lỗ hổng. Sự mất mát có thể bị hỏng dữ liệu, phá hủy hệ thống và/hoặc phương tiện, tiết lộ thông tin bí mật trái phép, giảm năng suất của nhân viên, v.v. Khi thực hiện phân tích rủi ro, nhóm nghiên cứu cũng phải xem xét tổn thất sau (*delayed loss*) khi đánh giá thiệt hại có thể xảy ra. Tổn thất sau có bản chất thứ cấp và diễn ra sau khi lỗ hổng được khai thác. Tổn thất sau có thể bao gồm thiệt hại cho danh tiếng, mất thị phần, chấp hành luật pháp v.v.

Ví dụ nếu máy chủ web bị tấn công và không hoạt động, thiệt hại ngay lập tức có thể là dữ liệu bị hỏng, thời gian cần thiết để máy chủ trở lại trực tuyến và thay thế bất kỳ đoạn mã hoặc thành phần nào cần thiết. Công ty có thể mất doanh thu nếu nhận các đơn đặt hàng và thanh toán qua trang web của mình. Nếu phải mất cả ngày để máy chủ web được khắc phục và trực tuyến trở lại, công ty có thể thiệt hại doanh số và lợi nhuận. Nếu mất cả tuần các máy chủ web ổn định và trực tuyến trở lại, công ty có thể mất lượng doanh thu và lợi nhuận đến mức không thể thanh toán các hóa đơn và chi phí khác. Đây sẽ là tổn thất sau. Nếu khách hàng của công ty mất niềm tin do hoạt động này, công ty có thể mất kinh doanh trong nhiều tháng hoặc nhiều năm. Đây là trường hợp cực kỳ nghiêm trọng của tổn thất sau.

Những loại vấn đề này làm cho quá trình định lượng chính xác thiệt hại mà các mối đe dọa cụ thể có thể gây phức tạp hơn song chúng phải được xem xét để đảm bảo thực tế cần được thể hiện trong phân tích kiểu này.

### 3.3.4 ***Phương pháp phân tích rủi ro***

a. *NIST SP 800-30*

NIST xây dựng cách phân tích rủi ro riêng, mô tả trong tài liệu SP 800-30, và được coi như tiêu chuẩn của chính phủ liên bang Mỹ. Phương pháp quản lý rủi ro của NIST chủ yếu tập trung vào các hệ thống máy tính và các vấn đề an ninh CNTT bao gồm các bước:

- Đặc trưng hệ thống
- Nhận dạng mối đe dọa
- Nhận dạng lỗ hổng
- Phân tích biện pháp kiểm soát
- Xác định mức độ chắc chắn
- Phân tích tác động
- Xác định rủi ro

- Khuyến nghị các biện pháp kiểm soát
- Lập tài liệu kết quả

Phương pháp này không bao gồm các loại mối đe dọa lớn như trong thiên tai, các vấn đề môi trường, hoặc các rủi ro an ninh liên quan đến rủi ro kinh doanh. Thay vào đó, phương pháp này tập trung vào các thành phần hoạt động của cơ quan/tổ chức và không nhất thiết phải là cấp độ chiến lược cao hơn. Phương pháp luận vạch ra các hành động cụ thể với các giá trị đầu vào và đầu ra liên quan.

b. *FRAP*

Phương pháp đánh giá rủi ro thứ hai được gọi là FRAP (*Facilitated Risk Analysis Process*). Điểm mấu chốt của phương pháp định tính này là chỉ tập trung vào các hệ thống thực sự cần đánh giá để giảm ràng buộc chi phí và thời gian. Phương pháp này nhấn mạnh các hoạt động kiểm tra trước để các bước đánh giá rủi ro chỉ được thực hiện trên các mục cần nhất. Phương pháp này được sử dụng để phân tích một hệ thống, ứng dụng hoặc quy trình nghiệp vụ tại một thời điểm. Dữ liệu được thu thập và các mối đe dọa đến hoạt động kinh doanh được ưu tiên dựa trên mức độ quan trọng của chúng. Nhóm đánh giá rủi ro ghi lại các biện pháp kiểm soát cần được đưa ra để giảm thiểu rủi ro được xác định cùng với các kế hoạch hành động để thực hiện các nỗ lực kiểm soát.

Phương pháp này không hỗ trợ việc tính khả năng bị khai thác hoặc kỳ vọng về tổn thất hàng năm. Mức độ nghiêm trọng của những rủi ro được xác định bởi kinh nghiệm của các thành viên trong nhóm. Tác giả của phương pháp này cho rằng cố gắng sử dụng các công thức toán học để tính toán rủi ro quá khó hiểu và tốn thời gian. Mục đích chính giữ cho quy mô của đánh giá nhỏ và các quy trình đánh giá đơn giản để nâng cao hiệu quả và giảm chi phí.

c. *OCTAVE*

OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) được sử dụng trong trường hợp người ta muốn quản lý và kiểm soát việc đánh giá rủi ro bên trong công ty. Phương pháp này được đưa ra bởi Viện Kỹ thuật phần mềm của Đại học Carnegie Mellon và được dự định sẽ được sử dụng trong các tình huống mà người quản lý đánh giá rủi ro cho an ninh thông tin trong công ty. Điều này cho phép những người làm việc bên trong cơ quan/tổ chức ở các vị trí lãnh đạo có thể đưa ra các quyết định liên quan đến cách tiếp cận tốt nhất để đánh giá tính an toàn của tổ chức của họ. Ý tưởng cơ bản của phương pháp này là những người làm việc hiểu rõ nhất những gì cần thiết và loại rủi ro nào họ phải đối mặt. Phạm vi đánh giá OCTAVE thường rất rộng so với cách tiếp cận tập trung hơn của FRAP. Trường hợp FRAP sẽ được sử dụng để đánh giá một hệ thống hoặc ứng dụng, OCTAVE sẽ được sử dụng để đánh giá tất cả các hệ thống, ứng dụng và quy trình nghiệp vụ trong tổ chức.

d. *FMEA*

FMEA (*Failure Modes and Effect Analysis*) xác định các chức năng, các lỗi chức năng, và đánh giá nguyên nhân lỗi và ảnh hưởng của các lỗi này tới các quy trình. Mục tiêu chính là xác định thứ mà chắc chắn gây lỗi và liệu có thể sửa chữa hay giảm thiểu ảnh hưởng. Phương pháp này thường được sử dụng trong phát triển sản phẩm và môi trường làm việc. Mục đích là để xác định vị trí mà bộ phận nào đó rất có thể bị trục trặc hoặc sửa chữa các sai sót mà có thể gây ra của trục trặc này hoặc thực hiện biện pháp kiểm soát để giảm tác động của lỗi.

FMEA trước hết được phát triển dành cho kỹ thuật hệ thống. Mục đích của nó là để kiểm tra những lỗi tiềm ẩn trong các sản phẩm và các quy trình liên quan đến chúng. Cách tiếp cận này được chứng minh là thành công và gần đây đã được điều chỉnh để sử dụng trong việc đánh giá các ưu tiên quản lý rủi ro và giảm thiểu các lỗ hổng đã biết. FMEA được sử dụng trong quản lý rủi ro vì mức độ chi tiết, các biến và độ phức tạp tiếp tục tăng lên khi các cơ quan/tổ chức hiểu được rủi ro ở các mức độ chi tiết hơn. Cách thức này cho phép xác định những cạm bẫy tiềm năng khi nhu cầu nhận biết về rủi ro được mở rộng.

e. *ISO 27005*

Bộ tiêu chuẩn ISO/IEC 27000 cung cấp  phương pháp luận phân tích rủi ro được tích hợp vào chương trình an toàn. ISO/IEC 27005 là tiêu chuẩn quốc tế về cách thức quản lý rủi ro được thực hiện trong khuôn khổ của một hệ thống quản lý an toàn thông tin (ISMS). Trong khi phương pháp luận rủi ro của NIST chủ yếu là CNTT và tập trung vào các hoạt động, phương pháp này đề cập đến CNTT và các vấn đề an toàn nhẹ nhàng hơn (tài liệu, an ninh nhân sự, đào tạo, v.v). Phương pháp này được tích hợp vào chương trình an toàn của cơ quan/tổ chức mà xử lý các mối đe dọa an toàn mà cơ quan/tổ chức có thể phải đối mặt.

## 3.4 Các chiến lược kiểm soát rủi ro

Khi xác định được các rủi ro, cơ quan/tổ chức phải quyết định cách xử lý chúng. Rủi ro có thể được xử lý theo bốn cách cơ bản:

- Chuyển/Chia sẻ rủi ro: sử dụng dịch vụ bảo hiểm
- Tránh: chấm dứt sử dụng dịch vụ gây rủi ro
- Giảm thiểu: làm mức độ nguy hiểm tới mức chấp nhận được như dùng tường lửa
- Chấp nhận: yêu cầu nhận thức rõ ràng về chi phí rủi ro/biện pháp phòng chống để có thể duy trì mức độ bảo vệ hiện thời.

Nếu cơ quan/tổ chức thấy rằng rủi ro tổng thể quá cao, họ có thể mua bảo hiểm, điều này sẽ chia sẻ/chuyển rủi ro cho công ty bảo hiểm. Nếu cơ quan/tổ chức quyết định chấm dứt hoạt động dẫn đến rủi ro, điều này được gọi là tránh rủi ro. Ví dụ, nếu một công ty

cho phép nhân viên sử dụng tin nhắn tức thì, có nhiều rủi ro xung quanh công nghệ này. Công ty có thể quyết định không cho phép bất kỳ hoạt động tin nhắn nào bởi người dùng của họ bởi vì không có nhu cầu đủ mạnh để tiếp tục sử dụng nó. Ngừng dịch vụ này là một ví dụ về tránh rủi ro.

Một cách tiếp cận khác là giảm thiểu rủi ro tức là rủi ro được giảm xuống mức đủ chấp nhận để cơ quan/tổ chức tiếp tục hoạt động. Việc triển khai tường lửa, đào tạo và hệ thống bảo vệ xâm nhập/phát hiện hoặc các biện pháp kiểm soát khác nhau là những nỗ lực để giảm thiểu rủi ro.

Cách tiếp cận cuối cùng là chấp nhận rủi ro, có nghĩa là cơ quan/tổ chức hiểu mức độ rủi ro mà họ phải đối mặt cũng như chi phí thiệt hại tiềm ẩn, và quyết định sống chung với rủi ro và không thực hiện biện pháp đối phó. Nhiều cơ quan/tổ chức sẽ chấp nhận rủi ro khi tỷ lệ chi phí/lợi ích cho thấy rằng chi phí của biện pháp đối phó lớn hơn giá trị tổn thất tiềm ẩn.

Một vấn đề quan trọng với việc chấp nhận rủi ro là hiểu nguyên nhân cho một tình huống cụ thể. Tuy vậy, nhiều tổ chức đang chấp nhận rủi ro và không hiểu đầy đủ những gì họ đang chấp nhận. Điều này thường phải làm với vấn đề mới của quản lý rủi ro trong lĩnh vực an ninh và thiếu đào tạo và kinh nghiệm trong những nhân viên đưa ra quyết định rủi ro. Khi các nhà quản lý buộc phải chịu trách nhiệm đối phó với rủi ro trong bộ phận của họ, hầu hết họ sẽ chấp nhận bất kỳ rủi ro phải đối mặt bởi vì mục tiêu thực sự của họ liên quan đến việc hoàn thành dự án. Họ không muốn bị sa lầy bởi những vấn đề an toàn khó chịu này.

Chấp nhận rủi ro nên dựa trên một số yếu tố. Ví dụ tổn thất thấp hơn so với biện pháp đối phó, cơ quan/tổ chức có thể chịu đựng được tổn thất của rủi ro. Các cá nhân hoặc nhóm chấp nhận rủi ro cũng phải hiểu viễn cảnh của quyết định này. Giả sử công ty không cần phải thực sự bảo vệ tên của khách hàng nhưng nó phải bảo vệ các thông tin khác như số CMND, số tài khoản, v.v. Vì vậy, các hoạt động hiện tại này tuân thủ các quy định và luật pháp nhưng nếu khách hàng của bạn phát hiện ra bạn không bảo vệ đúng tên của họ và họ gắn những điều đó với gian lận danh tính. Nhận thức về công ty của khách hàng không phải lúc nào cũng bắt nguồn từ thực tế nhưng khả năng khách hàng sẽ chuyển công việc của họ sang một công ty khác là một thực tế.

## 3.5 Các thực tế về kiểm soát rủi ro

### 3.5.1 *Lựa chọn biện pháp kiểm soát rủi ro*

Do các cơ quan/tổ chức có một loạt các mối đe dọa (không chỉ là vi rút máy tính và kẻ tấn công), mỗi loại mối đe dọa cần được giải quyết và lên kế hoạch một cách riêng biệt. Các cơ chế kiểm soát truy cập được sử dụng như các biện pháp bảo vệ an toàn. Các ứng dụng phần mềm và sự cố dữ liệu được cần được kiểm tra và áp dụng cách thức phát triển an toàn. Cũng như vậy, các vấn đề về mạng và viễn thông được phân tích và áp

dụng các biện pháp đảm bảo an toàn như tường lửa hay hệ thống phát hiện xâm nhập. Tất cả các đối tượng này đều có những rủi ro và yêu cầu lập kế hoạch liên quan.

Vấn đề là xác định và lựa chọn các biện pháp đối phó phù hợp cho các hệ thống. Việc này cung cấp các đặc trưng tốt nhất để xem xét và các kịch bản chi phí khác nhau để đánh giá khi so sánh các loại biện pháp đối phó khác nhau. Kết quả cuối cùng của việc phân tích các lựa chọn cho thấy biện pháp kiểm soát được chọn là thuận lợi nhất cho hoạt động của cơ quan/tổ chức.

a. *Lựa chọn biện pháp*

Biện pháp kiểm soát an toàn phải có ý nghĩa tốt với hoạt động của cơ quan/tổ chức tức là chi phí hiệu quả. Lợi ích của biện pháp cần lớn hơn chi phí để thực hiện nó. Cách tính toán chi phí/lợi ích thường được sử dụng cho biện pháp bảo vệ (kiểm soát) là:

*(Chi phí hàng năm trước khi thực hiện biện pháp bảo vệ) - (Chi phí hàng năm sau khi thực hiện biện pháp tự vệ) - (chi phí bảo vệ hàng năm) = giá trị bảo vệ*

Ví dụ, nếu chi phí cho mối đe doạ người bẻ khóa làm máy chủ không hoạt động là $12.000 trước khi triển khai bảo vệ được đề xuất và ước tính giá trị chi phí là $3.000 sau khi thực hiện biện pháp bảo vệ, trong khi chi phí bảo trì và hoạt động hàng năm của bảo vệ là $650 thì giá trị bảo vệ này cho công ty là $8.350 mỗi năm. Chi phí của một biện pháp đối phó không chỉ là số tiền được cấp mà cần xem xét các mục sau đây và đánh giá khi tính toàn bộ chi phí của biện pháp đối phó có thể bao gồm:

- Chi phí sản xuất
- Chi phí thiết kế / lập kế hoạch
- Chi phí triển khai
- Sửa đổi môi trường
- Khả năng tương thích với các biện pháp đối phó khác
- Yêu cầu bảo trì
- Yêu cầu kiểm tra
- Chi phí sửa chữa, thay thế hoặc cập nhật
- Chi phí hoạt động và hỗ trợ
- Ảnh hưởng đến năng suất
- Chi phí đăng ký

Nhiều cơ quan/tổ chức đã chấp nhận mua các sản phẩm bảo mật mới mà không hiểu rằng họ sẽ cần nhân viên để duy trì các sản phẩm đó. Mặc dù các công cụ tự động hóa các nhiệm vụ song nhiều cơ quan/tổ chức thậm chí chưa thực hiện các nhiệm vụ này trước đây vì vậy chúng không tiết kiệm thời gian làm việc và tiêu tốn nhân lực hơn.

Ví dụ để bảo vệ tài nguyên của công ty  công ty quyết định mua hệ thống thống phát hiện xâm nhập IDS. Công ty bỏ một khoản tiền cho IDS. Nhưng đó chưa phải chi phí cuối cùng cho biện pháp bảo vệ này. Phần mềm này cần được kiểm tra trong một môi trường tách biệt môi trường sản xuất để phát hiện bất kỳ hoạt động bất ngờ nào. Sau khi

thử nghiệm này hoàn tất và nhóm bảo mật cảm thấy an toàn khi chèn IDS vào môi trường sản xuất của mình, nhóm bảo mật phải cài đặt phần mềm quản lý giám sát, cài đặt bộ thu dữ liệu và cài đặt đường truyền từ bộ thu thập đến bộ điều khiển quản lý. Nhóm bảo mật cũng có thể cần phải cấu hình lại các bộ định tuyến để chuyển hướng luồng lưu lượng và chắc chắn cần đảm bảo rằng người dùng không thể truy cập vào bộ điều khiển quản lý IDS. Cuối cùng, nhóm bảo mật cần cấu hình một cơ sở dữ liệu để giữ tất cả các chữ ký tấn công và sau đó chạy các mô phỏng.

b. *Cân đối hiệu quả và chức năng*

Nhóm phân tích rủi ro phải đánh giá chức năng và hiệu quả của biện pháp bảo vệ. Khi chọn một biện pháp bảo vệ một số đặc trưng có thể ưu việt hơn các đặc trưng khác. Bảng dưới đây liệt kê và mô tả các đặc trưng cần được xem xét trước khi triển khai một cơ chế kiểm soát an toàn. Các biện pháp kiểm soát có thể cung cấp các đặc trưng ngăn chặn nếu chúng có khả năng hiển thị cao. Điều này thông báo với những kẻ bất lương tiềm năng về các biện pháp kiểm soát đầy đủ được triển khai.

**Bảng 3-2. Các đặc trưng các biện pháp kiểm soát**

| **Đặc trưng** | **Ý nghĩa** |
|---|---|
| Cung cấp bảo vệ thống nhất | Cấp độ bảo mật được áp dụng cho tất cả các cơ chế được thiết kế để bảo vệ theo phương pháp được chuẩn hóa. |
| Cung cấp chức năng ghi đè | Quản trị viên có thể ghi đè hạn chế nếu cần. |
| Đặc quyền tối thiểu mặc định | Khi được cài đặt, mặc định là quyền hạn chế thay vì cài đặt quyền kiểm soát tối đa với mọi người. |
| Độc lập với các biện pháp bảo vệ và tài sản | Biện pháp bảo vệ có thể được sử dụng để bảo vệ các tài sản khác nhau và các tài sản khác nhau có thể được bảo vệ bởi các biện pháp bảo vệ khác nhau. |
| Tính linh hoạt và bảo mật | Biện pháp bảo vệ càng an toàn thì càng tốt. Chức năng này nên có tính linh hoạt cho phép lựa chọn các chức năng khác nhau thay vì tất cả hoặc không có chức năng nào |
| Tương tác người dùng | Không làm người dùng lo lắng ảnh hưởng đến năng suất lao động |
| Chức năng kiểm toán | Nên có cơ chế là một phần của biện pháp tự vệ cung cấp kiểm toán tối thiểu và/hoặc chi tiết. |
| Giảm thiểu sự phụ thuộc vào các thành phần khác | Các biện pháp bảo vệ phải linh hoạt và yêu cầu không khắt khe về môi trường mà nó sẽ được cài đặt. |
| Dễ sử dụng và được nhân viên chấp nhận | Nếu các biện pháp bảo vệ cung cấp các rào cản đối với năng suất hoặc làm tăng thêm các bước thực hiện các nhiệm vụ đơn giản, người dùng sẽ không chịu đựng được. |

| | |
|---|---|
| Cung cấp các báo cáo và định dạng dễ hiểu | Thông tin quan trọng cần được trình bày ở định dạng dễ dàng để con người hiểu và sử dụng để phân tích xu hướng. |
| Phải có khả năng thiết lập lại biện pháp bảo vệ | Cơ chế bảo vệ có thể được thiết lập lại và trả về cấu hình và cài đặt ban đầu mà không ảnh hưởng đến hệ thống hoặc nội dung mà nó đang bảo vệ. |
| Thử nghiệm được | Các biện pháp bảo vệ có thể được kiểm tra ở các môi trường trong các tình huống khác nhau. |
| Không làm nảy sinh các lỗ hổng khác | Biện pháp bảo vệ không được cung cấp bất kỳ kênh bí mật nào hoặc cửa sau. |
| Hệ thống và hiệu suất của người dùng | Hiệu năng hệ thống và hiệu suất của người dùng sẽ không bị ảnh hưởng nhiều. |
| Không ảnh hưởng đến tài sản | Các tài sản trong hệ thống không phải chịu ảnh hưởng bất lợi bởi biện pháp bảo vệ. |

### 3.5.2 *Hệ thống kiểm soát rủi ro*

Các hệ thống kiểm soát rủi ro an toàn cung cấp các mô hình hay cấu trúc lô-gíc để hướng dẫn người quản lý các quy trình thực hiện đánh giá rủi ro với an toàn thông tin. Các hệ thống này thường không đi vào các chi tiết mà tập trung vào các khái niệm căn bản như các yếu tố rủi ro, các hành động hay tổ chức ...

Việc sử dụng hệ thống đánh giá tiêu chuẩn giúp công việc khởi thảo ban đầu ít hơn do các hệ thống tiêu chuẩn cung cấp đầy đủ tài liệu tham khảo cũng như dễ dàng bảo vệ hơn khi phải giải trình trước ban lãnh đạo cơ quan/tổ chức. Tuy nhiên, các hệ thống tiêu chuẩn này không phục vụ trực tiếp cho yêu cầu cụ thể của cơ quan/tổ chức và có các chi tiết rất khó hoặc không thể áp dụng được.

Với hệ thống đánh giá tự xây dựng, công việc khởi thảo ban đầu nhiều hơn do phải tự xây dựng từ đầu cách thức tính toán đánh giá, các hoạt động cũng như cách ra quyết định. Nếu người xây dựng có kiến thức vững chắc, hệ thống đánh giá hoàn toàn phù hợp với đặc điểm của cơ quan/tổ chức và sẽ dễ triển khai hơn, song khó giải trình và bảo vệ với lãnh đạo và quản lý

Phần dưới đây giới thiệu các hệ thống kiểm soát rủi ro thường được sử dụng trên thực tế:

- OCTAVE
- NIST
- ISO27005

### 3.5.3 *OCTAVE*

OCTAVE có 3 phiên bản:

- OCTAVE là hệ thống nguyên thủy và là cơ sở cho các phiên bản khác trong hệ thống OCTAVE. Hướng tới cơ quan/tổ chức lớn với hơn 300 nhân viên có đủ nguồn lực và khả năng thực hiện các đánh giá an toàn nội bộ.
- OCTAVE-S hướng tới cơ quan/tổ chức cỡ nhỏ thường ít hơn 100 nhân viên và cần nhóm 3-5 người có hiểu biết để thực hiện việc đánh giá về tài sản, yêu cầu an toàn, các mối đe dọa, thực hành an toàn
- OCTAVE-Allegro là phiên bản mới nhất hướng tới việc phổ biến rộng rãi việc đánh giá rủi ro an toàn thông tin

Các bước tiến hành OCTAVE bao gồm:

1. Thiết lập tiêu chuẩn đánh giá rủi ro
2. Xây dựng hồ sơ tài sản thông tin
3. Xác định đối tượng chứa tài sản
4. Xác định lĩnh vực quan tâm
5. Xác định các tình huống đe dọa
6. Xác định rủi ro
7. Phân tích rủi ro
8. Lựa chọn các tiếp cận giảm thiểu

Chi tiết các bước như phần dưới đây.

a. *Thiết lập tiêu chuẩn đánh giá rủi ro*

Bước này giúp nhóm phân tích nhận biết các lĩnh vực hay vấn đề chính có thể chịu tác động của các mối đe dọa. Các khía cạnh cần đánh giá như sau, trong đó tiêu chí cuối cùng do cơ quan/tổ chức tự xác định:

1. *Reputation/Customer Confidence* - Danh tiếng/Tín nhiệm của khách hàng
2. *Financial* - Tài chính
3. *Productivity* – Năng suất
4. *Safety and Health* – Sức khỏe và an toàn
5. *Fines and Legal Penalties* - Hình phạt và Phạt phạm luật
6. *User-defined Impact Criteria* – Tiêu chuẩn tác động riêng

b. *Xây dựng hồ sơ tài sản thông tin*

Mục tiêu là thu thập danh sách các tài sản dựa trên mức độ quan trọng. Các bước cơ bản bao gồm:

1. Lập hồ sơ chủ sở hữu
2. Cung cấp mô tả về tài sản quan trọng
3. Xác định các yêu cầu CIA (Bí mật-Toàn vẹn-Sẵn sàng)
4. Xây dựng yêu cầu CIA nào quan trọng nhất

5. Lý do về tính quan trọng của tài sản

c. *Xác định đối tượng chứa tài sản*

Thông tin thu thập có thể phân loại:

- Kỹ thuật : Phần cứng, quy trình, loại thông tin, ...
- Vật lý: Vị trí phần cứng hay dữ liệu, trung tâm dữ liệu...
- Con người: người sở hữu tài sản, Đầu mối kỹ thuật,...

d. *Xác định lĩnh vực quan tâm*

Bước này cần mô tả các chi tiết điều kiện hay tình huống thực tế có thể tác động lên tài sản của cơ quan/tổ chức. Về cơ bản bước này xác định các điểm yếu hay lỗ hổng có thể trong hệ thống.

e. *Xác định các tình huống đe dọa*

Mục tiêu tập trung vào các điều kiện xuất phát từ điểm yếu hay lỗ hổng tiềm tàng. Việc mô tả các tình huống bao gồm các yếu tố sau:

1.Tài sản

2.Truy nhập/Phương tiện

3.Người tiến hành

4.Động cơ

5.Kết quả

f. *Xác định rủi ro*

Bước này xây dựng danh sách các đe dọa và tác động dưới dạng:

*Rủi ro = Đe dọa (điều kiện) + Tác động (hậu quả)*

Bảng dưới đây cho một ví dụ về kết quả đánh giá.

**Bảng 3-3. Các rủi ro và ảnh hưởng.**

| **Đe dọa/Điểm yếu** | **Tác động** |
|---|---|
| Trên máy chủ Web, các lỗi về an toàn từ người phát triển có thể dẫn đến việc truy nhập trái phép từ người bẻ khóa bên ngoài | Trang web của công ty không chứa dữ liệu bí mật nhưng việc thay giao diện trang chủ hủy hoại danh tiếng của công ty và khách hàng tiềm năng đặt dấu hỏi về tính an toàn của toàn hệ thống |

g. *Phân tích rủi ro*

Việc phân tích tập trung chủ yếu vào tác động và thực hiện việc đánh giá kết hợp mức độ tác động và lĩnh vực ảnh hưởng như trong ví dụ ở bảng dưới đây.

**Bảng 3-4. Phân tích rủi ro**

| | **Phân loại** | **Giá trị tác động** | **Mức điểm** |
|---|---|---|---|
| Danh tiếng | 5 | Cao (3) | 15 |
| Tài chính | 3 | Thấp (1) | 3 |
| Năng suất | 4 | Trung bình (2) | 8 |
| An toàn và sức khỏe | 1 | Thấp (1) | 1 |
| Luật pháp | 2 | Thấp(1) | 2 |

h. *Lựa chọn giảm thiểu*

Các rủi ro được phân loại thành các nhóm:

1. Nhóm 1 – Giảm thiểu
2. Nhóm 2 – Giảm thiểu hay loại trừ
3. Nhóm 3 – Loại trừ hay chấp nhận
4. Nhóm 4 – Chấp nhận

Việc phân loại dựa vào kết quả đánh giá ở bước trước và xác suất xảy ra của mối đe dọa.

**Bảng 3-5. Đánh giá phương pháp**

| **Ưu điểm** | **Nhược điểm** |
|---|---|
| Tiết kiệm thời gian xây dựng các tài liệu bổ sung. Tài liệu, ma trận tiêu chí/quyết định, mẫu điều tra được cung cấp sẵn. | Cho dù OCTAVE-Allegro là phiên bản đơn giản hóa song nó vẫn khá dài và phức tạp |
| Việc mô tả được đơn giản hóa | Không xây dựng danh mục các mối đe dọa. Thay vào đó, OCTAVE sử dụng các mẫu điều tra mà chúng mang tính chủ quan. Với người thiếu kinh nghiệm có thể làm thiếu mối đe dọa |
| Cung cấp bảng các tiêu chí tác động. Cái này có ích cả với hệ thống khác | Việc chuẩn bị các tình huống đe dọa cho rằng người đánh giá có hiểu biết tốt về cơ quan và hệ thống |
| Các văn bản sử dụng khá dễ theo dõi | Việc điều chỉnh dựa trên kiểm soát không được tính toán rõ ràng. |

| | |
|---|---|
| Khái niệm nhóm và làm thế nào phân loại rủi ro là cơ sở tốt cho việc lựa chọn giảm thiểu | Tính chắc chắn không được tính toán rõ ràng và chỉ là một phần của lựa chọn giảm thiểu rủi ro |

### 3.5.4 ***NIST SP 800-30***

NIST SP 800-30 cung cấp tiếp cận mức cao cho việc quản lý rủi ro hướng tới cơ quan/tổ chức với các quy mô khác nhau. Các bước tiến hành bao gồm:

1. Mô tả đặc trưng hệ thống
2. Xác định đe dọa
3. Xác định lỗ hổng
4. Phân tích kiểm soát
5. Xác định mức độ chắc chắn
6. Phân tích tác động
7. Xác định rủi ro
8. Khuyến nghị các biện pháp kiểm soát
9. Lập báo cáo kết quả

Chi tiết các bước được trình bày như phần dưới đây.

a. *Mô tả đặc trưng hệ thống*

Bước này tập trung mô tả hệ thống hay tài sản trong phạm vi phân tích rủi ro. Mục tiêu là tạo cái nhìn tổng thể về hệ thống và môi trường hoạt động. Với mỗi tài sản cần các chi tiết như:

1. Phần cứng
2. Phần mềm
3. Giao tiếp
4. Dữ liệu & thông tin
5. Hỗ trợ con người
6. Nhiệm vụ
7. Mức độ quan trọng dữ liệu và hệ thống
8. Mức độ nhạy cảm dữ liệu và hệ thống

Các kỹ thuật có thể sử dụng để thu thập thông tin: Mẫu điều tra; Phỏng vấn tại chỗ; Xem xét tài liệu;Công cụ quét tự động.

b. *Xác định đe dọa*

Mục tiêu là xây dựng các mô tả về mối đe dọa có thể. Các mô tả này chứa thông tin về các nguồn đe dọa như người bẻ khóa. Danh sách các mô tả giúp cho người đánh giá có thể xác định nguồn đe dọa nào họ có thể tận dụng. Các nguồn này có thể được phân loại như tự nhiên, con người, hay môi trường.

c. *Xác định lỗ hổng*

Xác định các lỗ hổng ứng với các nguồn đe dọa mô tả ở bước trước. Thường được lưu thành 1 cặp: Nguồn đe dọa + lỗ hổng.

Tiếp theo là xác định hành động có thể với cặp thông tin này.

Các nguồn thông tin sau hỗ trợ cho việc xác định lỗ hổng:

1. Đánh giá rủi ro trước đó
2. Báo cáo kiểm toán hệ thống CNTT
3. Các danh sách lỗ hổng
4. Khuyến cáo an ninh
5. Khuyến cáo của nhà cung cấp
6. Trung tâm ứng cứu khẩn cấp
7. Kiểm tra an toàn hệ thống
8. Danh mục kiểm tra yêu cầu an toàn

d. *Phân tích các biện pháp kiểm soát*

Mục tiêu chính của bước này là xem xét các biện pháp kiểm soát hiện thời và sắp tới khi đánh giá mức độ chắc chắn về việc các lỗ hổng bị khai thác. SP 800-30 thảo luận các phương pháp kiểm soát, các loại biện pháp kiểm soát tuy nhiên cách hiệu quả hơn cả là tiến hành việc phân tích dựa trên các danh mục kiểm tra yêu cầu an toàn

e. *Xác định mức độ chắc chắn*

Tính toán xác suất mà lỗ hổng có thể bị khai thác từ các nguồn đe dọa. SP 800-30 phân thành 3 loại mức độ

1. *Cao:* Nguồn đe dọa có động cơ mạnh mẽ và khả năng đầy đủ và các biện pháp kiểm soát để ngăn chặn khai thác lỗ hổng không hiệu quả
2. *Vừa:* Nguồn đe dọa có động cơ và năng lực song các biện pháp kiểm soát hiện thời có thể cản trở việc khai thác thành công lỗ hổng
3. *Thấp*: Nguồn đe dọa thiếu động cơ hay khả năng hay các biện pháp kiểm soát hiện thời ngăn chặn hay cản trở đáng kể việc khai thác lỗ hổng.

f. *Phân tích tác động*

Xác định các tác động tiêu cực đến tài sản khi lỗ hổng bị tận dụng thành công từ nguồn đe dọa. SP 800-30 chia thành 3 mức độ tác động: Cao (Lớn), Vừa, Thấp.

Ví dụ tác động lớn: Việc lỗ hổng bị khai thác thành công có thể gây ra tổn thất lớn và tốn kém cho các tài sản dễ tổn thương; có thể xâm phạm, tổn hại hay cản trở đáng kể nhiệm vụ của cơ quan, danh tiếng; và có thể gây ra tổn thất về người hay bị thương nặng

g. *Xác định rủi ro*

Việc tính toán khá đơn giản theo công thức

*Rủi ro = Tác động x Độ chắc chắn*

**Bảng 3-6. Xác định mức độ rủi ro**

| **Độ chắc chắn** | **Tác động** | | |
|---|---|---|---|
| | Thấp(10) | Vừa(50) | Cao (100) |
| Cao (1.0) | Thấp 10x1 | Vừa 50x1 | Cao 100x1 |
| Vừa (0.5) | Thấp 0.5x10 | Vừa 50x0.5 | Vừa 100x0.5 |
| Thấp (0.1) | Thấp 0.1x10 | Thấp 50x0.1 | Thấp 100x0.1 |

h. *Khuyến nghị các biện pháp kiểm soát*

Các giải pháp đề xuất trên cơ sở xác định mức độ rủi ro phân tích được. NIST khuyên nên thực hiện đánh giá chi phí để chắc chắn các biện pháp kiểm soát có chi phí phù hợp với mức độ tổn thất.

i. *Lập báo cáo kết quả*

Báo cáo này tập hợp toàn bộ các báo cáo hay tóm tắt dựa trên đánh giá rủi ro. Tài liệu này giúp cho quản lý cấp cao có thể ra quyết định về chính sách, thủ tục, ngân sách cũng như các thay đổi về vận hành và quản lý. Các báo cáo này cần mô tả:

- Các nguồn đe dọa
- Các lỗ hổng
- Các rủi ro được đánh giá
- Các biện pháp kiểm soát đề xuất

**Bảng 3-7. Đánh giá phương pháp**

| **Ưu điểm** | **Nhược điểm** |
|---|---|
| Cung cấp hệ thống mở và mềm dẻo cho người quản lý | Kém khách quan và hướng dữ liệu so với các hệ thống khác |
| Cung cấp các mẫu câu hỏi phỏng vấn và báo cáo hữu ích | Thiếu các hướng dẫn về tiêu chí và quyết định. Các kết quả phân tích lệ thuộc vào kinh nghiệm và ý kiến của người quản lý/đánh giá |
| Nhiều tổ chức ở Mỹ, đặc biệt là cơ quan quốc gia, tuân thủ tiêu chuẩn này | Hướng dẫn ngắn gọn và rộng, không đủ chi tiết. Các ví dụ triển khai rời rạc |
| Thảo luận tốt về khái niệm đe dọa và lỗ hổng.<br>Phần giảm thiểu rủi ro rất chi tiết và có ích với triển khai quản lý rủi ro<br>Đầu vào và ra của các bước rõ ràng | Các nguồn đe dọa chủ yếu phục vụ cho các cơ quan quân đội và chính phủ. |

### 3.5.5 *ISO 27005*

Đây hệ thống kiểm soát do Tổ chức tiêu chuẩn quốc tế ISO đưa ra nhằm cung cấp các hướng dẫn về các quy trình quản lý rủi ro an toàn thông tin cần thiết cho việc triển khai hệ thống quản lý an toàn thông tin hiệu quả. Bao gồm 6 chủ đề chính

1. Xây dựng ngữ cảnh
2. Đánh giá rủi ro an toàn thông tin
3. Xử lý rủi ro an toàn thông tin
4. Chấp nhận rủi ro an toàn thông tin
5. Truyền thông về rủi ro an toàn thông tin
6. Xem xét lại và giám sát rủi ro an toàn thông tin

ISO 27005 có 3 bước xử lý việc đánh giá rủi ro bao gồm xác định, ước lượng và đánh giá rủi ro.

a. *Xác định rủi ro*

Việc xác định rủi ro gồm các bước sau:

1. Xác định tài sản: nhận biết các tài sản trong phạm vi đánh giá
2. Xác định mối đe dọa: Lập danh sách các mối đe dọa tiềm tàng
3. Xác định các biện pháp kiểm soát hiện thời
4. Xác định lỗ hổng: sử dụng việc kiểm tra xâm nhập hay quét lỗ hổng, Mẫu điều tra ...
5. Xác định hậu quả:

b. *Ước lượng rủi ro*

Mục đích của bước này mục đích là đánh giá hậu quả bao gồm:

- Đánh giá tác động của sự kiện. Một số tiêu chí sử dụng như thời gian điều tra và sửa chữa, thời gian làm việc bị mất, phí tổn để sửa chữa,...
- Đánh giá mức độ chắc chắn của sự kiện: sử dụng biện pháp định lượng và định tính như: tần suất xuất hiện của mối đe dọa, động cơ và khả năng của nguồn đe dọa
- Mức độ ước lượng rủi ro: cho biết số đo mức độ chắc chắn và hậu quả

c. *Đánh giá rủi ro*

Ngay sau khi xác định rủi ro, người quản lý cần phân loại ưu tiên các rủi ro và trên cơ sở đó xác định hành động cần thiết.

**Bảng 3-8. Đánh giá phương pháp**

| Ưu điểm | Nhược điểm |
|---|---|
| ISO 27005 cung cấp các thông tin và ví dụ hữu ích như danh mục đe dọa, lỗ hổng các kỹ thuật tính toán và xếp loại rủi ro | Cách diễn giải mở dẫn đến các cơ quan khác nhau có cách hiểu và thực hiện khác nhau |

| | |
|---|---|
| ISO là tổ chức lớn và được công nhận<br>ISO 27005 mềm dẻo và có thể triển khai thuận tiện | |

## 3.6 Câu hỏi ôn tập

1. Phân tích các dạng rủi ro cơ bản.
2. Trình bày các yêu cầu với nhóm thực hiện quản lý rủi ro.
3. Giải thích sự khác biệt giữa đánh giá rủi ro và phân tích rủi ro.
4. Trình bày các cách thức xử lý rủi ro cơ bản? Cho ví dụ.
5. Trình bày ưu nhược điểm các cách thức đánh giá và phân tích rủi ro NIST SP 800-30, OCTAVE và ISO 27005.
6. Lần lượt áp dụng các hệ thống kiểm soát rủi ro OCTAVE, NIST, ISO 27005 để thực hiện các bước đánh giá và phân tích rủi ro cho hệ thống thương mại điện tử hay một hệ thống máy tính nào khác.

# CHƯƠNG 4. HỆ THỐNG TIÊU CHUẨN AN TOÀN THÔNG TIN

Trên thực tế, không ai chọn một tiêu chuẩn an toàn và triển khai chỉ vì những ích lợi của tiêu chuẩn đó. Thay vào đó, cần phải xem xét bối cảnh của cơ quan/tổ chức cùng với những mục tiêu hoạt động thiết yếu đó trong phạm vi pháp lý, việc chấp hành các quy định và các rủi ro mà cơ quan hoạt động. Tiêu chuẩn an toàn, do đó, phải được sử dụng đúng cách. Nếu động cơ để thực hiện tiêu chuẩn chỉ đơn giản là chứng minh việc tuân thủ, cách tiếp cận này sẽ giúp cho việc hoàn tất danh sách kiểm tra của kiểm toán và đủ để có được chứng nhận nhưng không loại trừ được các rủi ro về an toàn. Điều quan trọng là hệ thống quản lý an toàn thông tin là một phần tích hợp với các quy trình của tổ chức và cấu trúc quản lý. Bên cạnh đó, an toàn thông tin đó cần được xem xét trong thiết kế các quy trình, hệ thống thông tin và các biện pháp kiểm soát.

Điều tối quan trọng là phải xem xét tất cả các tiêu chuẩn an toàn, hướng dẫn thực hành tốt nhất và khung công việc và biến chúng thành của riêng cơ quan/tổ chức. Tiêu chuẩn phải được tích hợp trong hệ thống quản lý chất lượng của cơ quan/tổ chức để đảm bảo rằng nó được duy trì và tiếp cận, có nghĩa là cần phải cân nhắc việc căn chỉnh cấu trúc tài liệu theo yêu cầu của bộ tiêu chuẩn được chọn.

Chương này trình bày về các tiêu chuẩn về an toàn thông tin phổ biến trên thế giới do Tổ chức tiêu chuẩn quốc tế ISO, Viện Tiêu chuẩn và Công nghệ Quốc gia Mỹ NIST ban hành. Nội dung chủ yếu giới thiệu bộ tiêu chuẩn IS0 27000 và hệ thống tiêu chuẩn NIST. Phần cuối chương giới thiệu các tiêu chuẩn về an toàn thông tin của Việt Nam đã được công bố.

## 4.1 Hệ thống tiêu chuẩn an toàn thông tin trên thế giới

Tiêu chuẩn là các tài liệu đã được xuất bản bởi một tổ chức được công nhận, chẳng hạn như Tổ chức tiêu chuẩn quốc tế (ISO). Các tài liệu này giúp truyền đạt sự hiểu biết chung về các đặc điểm và quy trình cần thiết để đảm bảo việc cung cấp các sản phẩm và dịch vụ đáng tin cậy. Các tiêu chuẩn thường chi tiết các cách thức và các yêu cầu của một sản phẩm hay kết quả cụ thể, chẳng hạn như trong trường hợp hệ thống quản lý an toàn thông tin, để cho việc tích hợp được nhất quán vào bất kỳ tổ chức cụ thể nào.

Từ quan điểm của người quản lý an toàn thông tin, các tiêu chuẩn an toàn cung cấp các mô hình tham chiếu cơ bản để phát triển các khả năng bảo mật bằng cách thiết lập các biện pháp nhất quán để cung cấp các biện pháp kiểm soát an toàn mà chúng được hiểu và chấp nhận trong toàn bộ cơ quan/tổ chức. Các tiêu chuẩn cũng giúp người dùng cung cấp các hệ thống có thể được kiểm chứng một cách độc lập phù hợp với mục tiêu và cho phép các cơ quan/tổ chức được bảo đảm rằng họ đang thực hiện các biện pháp đáp ứng các yêu cầu về luật pháp và thương mại.

Các tiêu chuẩn có thể cung cấp nhiều lợi ích mà người quản lý an toàn nên xem xét:

- Tiêu chuẩn có thể được sử dụng để chứng minh cho khách hàng rằng cơ quan/tổ chức nghiêm túc về an ninh
- Các tiêu chuẩn có thể cho phép phối hợp tốt hơn các thay đổi về tổ chức với tất cả các bên liên quan vì việc thực hiện một tiêu chuẩn sẽ thường bắt buộc việc tuân thủ với toàn bộ nhân sự
- Tiêu chuẩn cũng có thể được áp dụng như một yêu cầu đối với các nhà cung cấp để giúp tăng cường an ninh cho chuỗi cung ứng
- Sản phẩm và dịch vụ được chứng nhận tuân thủ các tiêu chuẩn an toàn có thể đạt được lợi thế cạnh tranh vì khách hàng sẽ luôn cảm thấy tự tin
- Tiêu chuẩn có thể giúp biện pháp kiểm soát và xử lý an toàn nội bộ của cơ quan phù hợp với các đối tác, khách hàng và chính phủ khiến cho công việc trở nên dễ dàng hơn

Tôn trọng các tiêu chuẩn, trong nhiều trường hợp tuân thủ các quy định, cần thiết để tăng sự thu hút với thị trường. Điều quan trọng là nhận biết về các tổ chức có ảnh hưởng nhất phát triển và duy trì các tiêu chuẩn chi phối các khía cạnh khác nhau của tính toán và truyền thông mạng. Phần dưới đây giới thiệu một số các tổ chức có ảnh hưởng trên thế giới về phát triển và duy trì các tiêu chuẩn cho an toàn thông tin.

### 4.1.1 *NIST*

Viện Tiêu chuẩn và Công nghệ Quốc gia, NIST (*National Institute of Standards and Technology*), là một cơ quan liên bang trong Bộ Thương mại Hoa Kỳ. Thành lập năm 1901 với tư cách là Cục Tiêu chuẩn Quốc gia, NIST là phòng thí nghiệm nghiên cứu khoa học vật lý liên bang đầu tiên của Mỹ. Sứ mệnh của NIST là "thúc đẩy sự đổi mới của Hoa Kỳ và khả năng cạnh tranh công nghiệp bằng cách thúc đẩy khoa học đo lường, tiêu chuẩn và công nghệ theo những cách tăng cường an ninh kinh tế và nâng cao chất lượng cuộc sống". NIST cung cấp các tiêu chuẩn về đo lường và công nghệ mà gần như tất cả các thiết bị máy tính đều dựa vào. Mặc dù, NIST là một cơ quan không quản lý, nhiều tổ chức tôn trọng và áp dụng các ấn phẩm của NIST. NIST thực hiện nhiệm vụ chính của mình thông qua bốn chương trình hợp tác:

- Các phòng thí nghiệm của NIST: Các phòng thí nghiệm tiến hành nghiên cứu để thúc đẩy cơ sở hạ tầng công nghệ của Hoa Kỳ. Ngành công nghiệp của quốc gia sử dụng cơ sở hạ tầng này để nâng cao chất lượng sản phẩm và dịch vụ.
- Chương trình Chất lượng Quốc gia Baldrige: Chương trình quốc gia trao quyền và khuyến khích sự xuất sắc trong các tổ chức của Hoa Kỳ bao gồm nhà sản xuất, tổ chức dịch vụ, tổ chức giáo dục, nhà cung cấp dịch vụ chăm sóc sức khỏe và tổ chức phi lợi nhuận. Cơ quan này cũng phấn đấu để tăng chất lượng và công nhận các tổ chức đạt được mục tiêu chất lượng.

- Đối tác sản xuất Hollings - Quan hệ đối tác này là một mạng lưới các trung tâm trên toàn quốc cung cấp hỗ trợ kỹ thuật và kinh doanh cho các nhà sản xuất vừa và nhỏ.
- Chương trình đổi mới công nghệ - Một chương trình quốc gia khác cung cấp giải thưởng cho các tổ chức và trường đại học để hỗ trợ các công nghệ mang tính cách mạng có thể áp dụng cho các nhu cầu quan trọng của lợi ích quốc gia.

NIST duy trì các tiêu chuẩn và ấn phẩm về lợi ích chung cho cộng đồng an toàn máy tính. NIST đã thiết lập tập hợp tài liệu này, được gọi là loạt ấn phẩm đặc biệt dòng 800 vào năm 1990 để đảm bảo đặc trưng riêng biệt cho an toàn công nghệ thông tin. Các ấn phẩm này công bố các nỗ lực nghiên cứu và hướng dẫn về vấn đề an toàn máy tính trong các cơ quan chính phủ, ngành công nghiệp và giảng dạy.

### 4.1.2 *ISO*

Tổ chức tiêu chuẩn hóa quốc tế (ISO) được thành lập năm 1946. Đây là một tổ chức quốc tế phi chính phủ. Mục tiêu của nó là phát triển và xuất bản các tiêu chuẩn quốc tế. ISO, có trụ sở tại Geneva, Thụy Sĩ, là một mạng lưới gồm 163 viện tiêu chuẩn quốc gia. ISO là cầu nối giữa khu vực công và tư nhân. Một số thành viên là các tổ chức chính phủ, trong khi số khác thuộc khu vực tư nhân. Mục tiêu của ISO là phát triển các tiêu chuẩn không phục vụ riêng biệt cho nhóm nào mà cần đạt được sự đồng thuận. ISO phấn đấu cho sự đồng thuận, ngay cả trong việc lựa chọn tên của tổ chức này. Việc tập trung vào sự đồng thuận khiến cho ISO thành công trong việc phát triển và thúc đẩy các tiêu chuẩn trong nhiều lĩnh vực.

ISO công bố nhiều tiêu chuẩn cho gần như tất cả các ngành công nghiệp ví dụ như số sách tiêu chuẩn quốc tế (ISBN) là tiêu chuẩn ISO. Đối với những người trong công nghệ thông tin, có lẽ tiêu chuẩn ISO nổi tiếng nhất là mô hình tham chiếu OSI (*Open Systems Interconnection*). Khung tiêu chuẩn được quốc tế chấp nhận này điều chỉnh cách các hệ thống máy tính riêng biệt giao tiếp bằng cách sử dụng mạng.

### 4.1.3 *ICE*

Ủy ban Kỹ thuật Điện Quốc tế IEC (International Electrotechnical Commission) là một tổ chức tiêu chuẩn thường làm việc chặt chẽ với ISO. IEC là tổ chức ưu việt cho việc phát triển và xuất bản các tiêu chuẩn quốc tế về công nghệ liên quan đến các thiết bị và quy trình điện và điện tử. Tổ chức này được thành lập vào năm 1906 để giải quyết các vấn đề với các công nghệ mở rộng liên quan đến các thiết bị điện. Ngày nay, các tiêu chuẩn của IEC đề cập đến nhiều lĩnh vực, bao gồm:

- Phát điện
- Truyền tải và phân phối điện
- Thiết bị điện thương mại và tiêu dùng
- Chất bán dẫn

- Điện từ
- Pin
- Năng lượng mặt trời
- Viễn thông

Để đảm bảo sự chấp nhận quốc tế và sử dụng tối đa các tiêu chuẩn của mình, IEC khuyến khích sự tham gia của nhiều quốc gia nhất có thể. Tổ chức này có 72 thành viên đầy đủ, cũng được gọi là Ủy ban Quốc gia (NC), trong IEC. Năm 2001, IEC mở rộng thành viên của mình để bao gồm nhiều quốc gia đang phát triển hơn. Chương trình quốc gia liên kết bao gồm 81 quốc gia nhỏ hơn.

Trọng tâm của IEC đã mở rộng kể từ khi thành lập, khi các ngành công nghiệp điện và điện tử đã thay đổi. Trong lĩnh vực CNTT, rất có thể sẽ gặp phải các tiêu chuẩn IEC liên quan đến phần cứng máy tính và phần cứng mạng. Ngày nay, phần lớn trọng tâm của IEC bao gồm các tiêu chuẩn giải quyết các nhu cầu năng lượng mới nổi và cách chúng ảnh hưởng đến các khu chức năng khác. IEC đang hoạt động trong việc phát triển các tiêu chuẩn hỗ trợ an toàn, hiệu suất, trách nhiệm môi trường, hiệu quả năng lượng và các nguồn năng lượng tái tạo và sử dụng.

### 4.1.4 *IEEE*

Viện Kỹ sư Điện và Điện tử IEEE (*Institute of Electrical and Electronics Engineers*) là "hiệp hội chuyên nghiệp lớn nhất thế giới về sự tiến bộ của công nghệ". Đây là một tổ chức phi lợi nhuận quốc tế tập trung phát triển và phân phối các tiêu chuẩn liên quan đến điện và điện tử. Với hơn 380.000 thành viên ở khoảng 175 quốc gia, nó có số lượng thành viên lớn nhất của bất kỳ tổ chức kỹ thuật chuyên nghiệp nào trên thế giới. IEEE được thành lập vào năm 1963 thông qua việc sáp nhập của hai tổ chức lớn tuổi hơn: Viện Kỹ sư Radio, được thành lập năm 1912 và Viện Kỹ sư Điện Hoa Kỳ, được thành lập vào năm 1884.

IEEE hỗ trợ 38 cộng đồng tập trung vào các lĩnh vực kỹ thuật cụ thể bao gồm từ tính, quang phổ và máy tính. Mỗi cộng đồng phát triển các ấn phẩm, tổ chức các hội nghị, và thúc đẩy các hoạt động và sự kiện để nâng cao kiến thức và sự quan tâm trong một lĩnh vực cụ thể. IEEE cũng cung cấp nhiều cơ hội đào tạo và giáo dục bao gồm một số lớn các chủ đề kỹ thuật. IEEE cũng là một trong những tổ chức sản xuất tiêu chuẩn lớn nhất. Các tiêu chuẩn IEEE bao gồm nhiều ngành, bao gồm cả công nghệ thông tin. IEEE hiện đang xuất bản hoặc tài trợ hơn 1.300 tiêu chuẩn và dự án. Tiêu chuẩn nổi tiếng nhất liên quan đến bảo mật thông tin là họ tiêu chuẩn IEEE 802 LAN/MAN. Nhóm tiêu chuẩn này xác định cách các loại mạng cục bộ (LAN) và giao thức mạng khu vực đô thị (MAN) hoạt động như thế nào. IEEE dành cho các thành viên từ cộng đồng kỹ thuật đáp ứng các yêu cầu nghề nghiệp nhất định. Các thành viên đầy đủ có thể bỏ phiếu trong cuộc bầu cử IEEE.

### 4.1.5 *IETF*

Nhóm kỹ thuật Internet IETF (*Internet Engineering Task Force*) phát triển và thúc đẩy các tiêu chuẩn Internet với mục đích "làm cho Internet hoạt động tốt hơn". IETF tập trung vào các khía cạnh kỹ thuật của truyền thông Internet và cố gắng tránh các chất vấn về chính sách và kinh doanh. IETF hoạt động chặt chẽ với W3C và ISO, tập trung chủ yếu vào các tiêu chuẩn của bộ giao thức TCP/IP hoặc Internet. IETF là một tổ chức mở và không yêu cầu hội viên. Tất cả những người tham gia, kể cả những người đóng góp và lãnh đạo, đều là tình nguyện viên.

IETF lần đầu tiên gặp mặt vào năm 1986 với tư cách là một nhóm gồm 21 nhà nghiên cứu muốn chính thức hóa các giao thức truyền thông Internet chính. Ngày nay, IETF là một tập hợp các nhóm làm việc WG, với mỗi nhóm giải quyết một chủ đề cụ thể. Hiện tại có hơn 100 WG. Bởi vì WG có xu hướng hoạt động độc lập, IETF đặt ra các tiêu chuẩn tối thiểu cho mỗi nhóm. Mỗi WG có một vị trí hoặc một nhóm đồng chủ tịch và một điều lệ để ghi lại sự tập trung của nhóm và các báo cáo dự kiến. Mỗi WG có một danh sách gửi thư chuyên dụng mà bất kỳ ai cũng có thể tham gia. Các danh sách gửi thư WG này đóng vai trò là phương tiện truyền thông chính cho những người tham gia. WG tổ chức các cuộc họp định kỳ và mở cho tất cả những người tham gia ngoài việc chỉ tương tác thông qua danh sách gửi thư.

Các yêu cầu thảo luận RFC (*Request for Comments*) được IETF tạo ra. Thực tế, RFC là một loạt các tài liệu từ các bản ghi nhớ đơn giản đến các tài liệu tiêu chuẩn. Mỗi phần giới thiệu của RFC cho biết trạng thái của nó. Mô hình RFC cho phép đầu vào từ nhiều nguồn và khuyến khích cộng tác và đánh giá ngang hàng. IETF xuất bản hướng dẫn cho RFC. Dưới đây là một vài điểm về RFC:

- Chỉ một số RFC là tiêu chuẩn: Chỉ các tài liệu RFC bắt đầu với các cụm từ như "Tài liệu này chỉ định ..." hoặc "Tài liệu ghi nhớ này ..." phải được coi là tiêu chuẩn hoặc tài liệu quy phạm.
- RFC không bao giờ thay đổi: Bất kỳ thay đổi nào đối với RFC đều có số mới và trở thành RFC mới vì vậy luôn tìm tài liệu RFC mới nhất.
- RFC có thể bắt nguồn từ các tổ chức khác: IETF chỉ tạo ra một số RFC. những tài liệu khác có thể đến từ các nguồn độc lập như ITTF(Internet Task Task Force).
- RFC xác định các tiêu chuẩn chính thức có bốn giai đoạn. Khi RFC chuyển từ giai đoạn này sang giai đoạn tiếp theo, nó trở nên chính thức hơn và nhiều tổ chức hơn chấp nhận nó. Các giai đoạn như sau:
  - Tiêu chuẩn đề xuất: Giai đoạn chính thức ban đầu của tiêu chuẩn
  - Tiêu chuẩn dự thảo: Giai đoạn thứ hai của tiêu chuẩn, sau khi người tham gia đã chứng minh rằng tiêu chuẩn đã được triển khai trong môi trường làm việc

- Tiêu chuẩn: Giai đoạn cuối của tiêu chuẩn sau khi nó chứng tỏ được việc chấp nhận và triển khai một cách rộng rãi.
- Thực tiễn tối ưu: các cách thức khác được áp dụng trong các thực tiễn vận hành mà không phải là các tiêu chuẩn chính thức.

#### 4.1.6 *PCI DSS*

Tiêu chuẩn bảo mật dữ liệu thẻ thanh toán PCI-DSS (*Payment Card Industry Data Security Standard*) là tiêu chuẩn quốc tế để xử lý các giao dịch liên quan đến thẻ thanh toán. Hội đồng tiêu chuẩn bảo mật thẻ thanh toán (PCI SSC) đã phát triển, xuất bản và duy trì tiêu chuẩn. PCI DSS khác với các tiêu chuẩn khác do một số nhà cung cấp thẻ thanh toán lớn nhất trên thế giới lập nên PCI DSS. Những nhà cung cấp này bao gồm Visa, MasterCard, Discover, American Express, Cục Tín dụng Nhật Bản.

Mỗi tổ chức này đều có tiêu chuẩn riêng để bảo vệ thông tin thẻ thanh toán. Các tổ chức này đã kết hợp những nỗ lực của mình và công bố PCI DSS vào tháng 12/2004 để bảo vệ người dùng thẻ thanh toán khỏi gian lận. Nó đòi hỏi các lớp điều khiển để bảo vệ tất cả các thông tin liên quan đến thẻ thanh toán khi được xử lý, truyền và lưu trữ. Tiêu chuẩn này áp dụng cho tất cả các tổ chức tham gia vào bất kỳ quy trình nào xung quanh việc xử lý thẻ thanh toán.

Việc tuân thủ các tiêu chuẩn PCI DSS là điều kiện tiên quyết để làm kinh doanh với bất kỳ tổ chức thành viên nào. Nếu bất kỳ tổ chức nào vi phạm tiêu chuẩn PCI DSS, nó có thể mất khả năng xử lý thẻ thanh toán của mình. Trong hầu hết các trường hợp, việc không tuân thủ dẫn đến tiền phạt và/hoặc kiểm toán thường xuyên hơn. Những người vi phạm có thể bị thu hồi các đặc quyền xử lý của họ. Đối với hầu hết các tổ chức phụ thuộc vào thẻ thanh toán là phương thức nhận thanh toán, việc tuân thủ là yêu cầu kinh doanh.

### 4.2 Hệ thống tiêu chuẩn ISO/IEC

#### 4.2.1 *ISO 17799*

An toàn hoàn hảo chỉ có thể đạt được khi các máy chủ không nối mạng nằm trong các phòng khép kín hoàn toàn. an toàn thông tin luôn là vấn đề cân nhắc các lựa chọn và cân bằng các yêu cầu hoạt động đối với bộ ba: bí mật, tính toàn vẹn và tính sẵn dùng. Quy trình an toàn thông tin theo truyền thống dựa trên các nguyên tắc và hướng dẫn chặt chẽ và tốt nhất với mục tiêu là ngăn chặn, phát hiện các vi phạm an ninh, và khôi phục dữ liệu bị ảnh hưởng về trạng thái trước đó. ISO 17799 cung cấp cách thức đo lường với các biện pháp xây dựng an toàn thông tin cơ quan/tổ chức. Nó cũng cung cấp một cơ chế để quản lý quá trình bảo mật thông tin. Đây là một trong những mô hình được tham chiếu rộng rãi nhất và thường được thảo luận là "*Information Technology – Code of Practice for Information Security Management"*, được công bố đầu tiên British Standard 7799. Quy định này được dùng làm chuẩn quốc tế bởi ISO và IEC dưới tên ISO/IEC 17799 vào

năm 2000 như là khung cho an toàn thông tin. Một số nước không làm theo chuẩn 17799 và cho rằng có những vấn đề cơ bản sau:

- Cộng đồng an toàn thông tin toàn cầu vẫn chưa xác định lý lẽ cho quy định được mô tả trong ISO/IEC 17799
- 17799 thiếu "sự chính xác của các biện pháp cần thiết của một chuẩn kỹ thuật"
- Không có lý do để tin rằng 17799 hữu dụng hơn các biện pháp khác hiện có.
- 17799 chưa hoàn chỉnh như các khung kỹ thuật khác hiện có
- 17799 được cho là chuẩn bị vội vã vì ảnh hưởng nó lên việc kiểm soát ngành công nghiệp an toàn thông tin

ISO 17799 hướng tới các mục tiêu cơ bản như sau:

- Hạ tầng an toàn tổ chức:
  - Quản lý an toàn thông tin bên trong tổ chức
  - Duy trì an toàn các phương tiện xử lý thông tin và các tài sản thông tin được truy nhập bởi bên thứ 3
  - Duy trì an toàn thông tin khi trách nhiệm xử lý thông tin được thuê ngoài tới cơ quan hay tổ chức khác
- An toàn nhân sự:
  - Giảm thiểu rủi ro do lỗi con người, trộm cắp, lừa đảo hay lạm dụng thiết bị
  - Đảm bảo người dùng nhận thức các đe dọa và quan tâm về an toàn thông tin và được trang bị để hỗ trợ chính cách an toàn của cơ quan trong quá trình làm việc hàng ngày.
  - Giảm thiểu tổn hại từ các sự kiện an toàn và trục trặc và học hỏi từ những sự kiện như vậy
- An toàn vật lý và môi trường
  - Ngăn chặn truy nhập trái phép, hư hỏng và gián đoạn tài sản và thông tin của cơ quan
  - Ngăn chặn mất mát, hư hỏng hay tổn hại tài sản và gián đoạn các hoạt động của cơ quan
  - Ngăn chặn hư hại hay mất cắp thông tin và các phương tiện xử lý thông tin.
- Quản lý hoạt động và liên lạc
  - Đảm bảo việc hoạt động an toàn và đúng đắn của các phương tiện xử lý thông tin
  - Tối thiểu rủi ro lỗi hệ thống
  - Bảo vệ tính toàn vẹn của phần mềm và thông tin

- Duy trì tính toàn vẹn và sẵn sàng của việc xử lý thông tin và liên lạc
- Đảm bảo việc bảo vệ thông tin trong mạng và hạ tầng hỗ trợ
- Ngăn chặn tổn hại tới tài sản và gián đoạn các hoạt động kinh doanh
- Ngăn chặn việc mất mát, sửa đổi hay dùng sai thông tin trao đổi giữa các cơ quan

▪ Tuân thủ/Phù hợp

- Tránh xung đột với bất kỳ luật hình sự/dân sự, quy định, bắt buộc trong hợp đồng hay bất kỳ yêu cầu an ninh nào
- Đảm bảo hệ thống tuân thủ các chính sách và tiêu chuẩn an toàn của cơ quan
- Tối đa hiệu quả và tối thiểu can thiệp vào/từ quy trình kiểm toán hệ thống

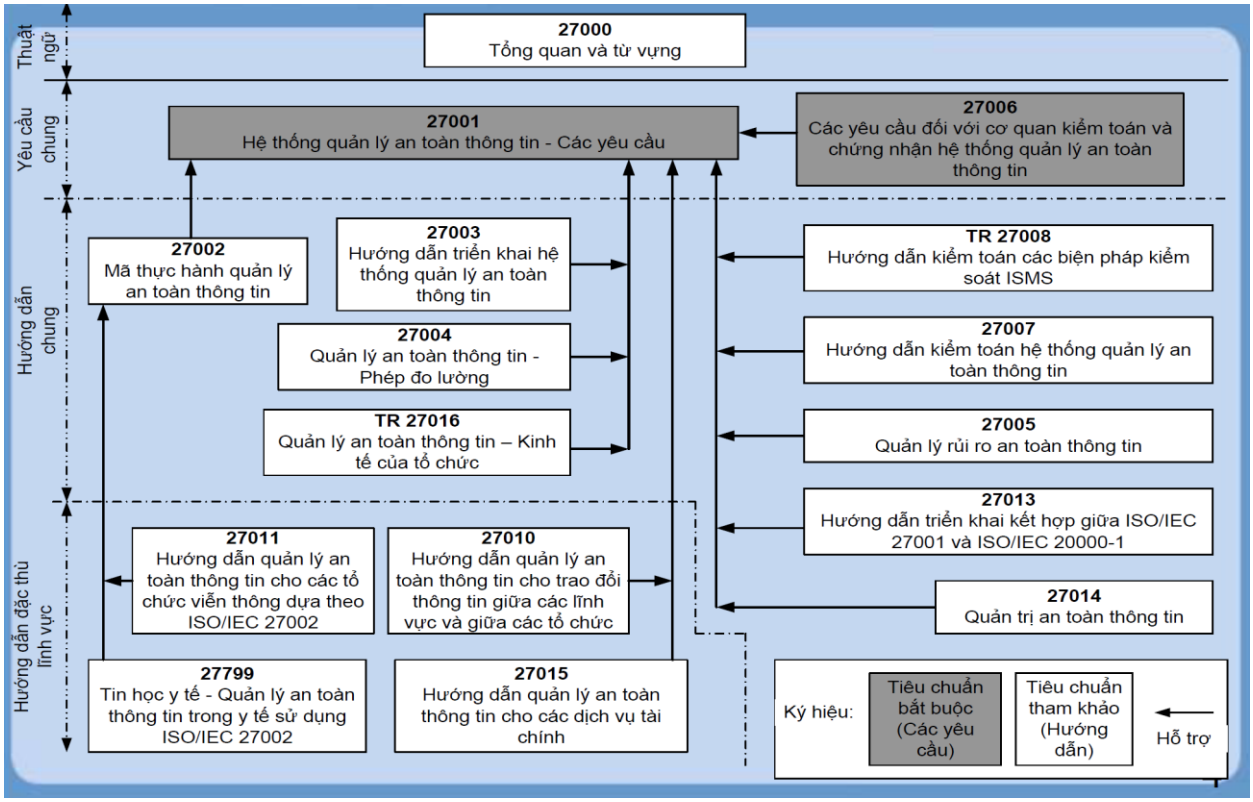
### 4.2.2 *Bộ tiêu chuẩn ISO 27000*

Loạt tiêu chuẩn trong bộ ISO/IEC 27000 bao gồm một loạt các khuyến nghị quản lý an toàn và thực tiễn tốt nhất có thể được áp dụng để giúp xây dựng một hệ thống quản lý an toàn thông tin ISMS (*Information Security Management System*). Nhiều người lạm dụng thuật ngữ ISMS cho rằng đây là một tài liệu hoặc tập hợp các tài liệu chi tiết về tất cả vấn đề an toàn của cơ quan/tổ chức. Điều này đúng một phần song bỏ qua thực tế là, giống như bất kỳ mô hình quy trình nào khác, nó có thể được áp dụng cho bất kỳ quy trình nào và sẽ được xây dựng và phát triển trong ngữ cảnh của cơ quan/tổ chức cho đến khi mô hình này hoàn thiện.

Tương tự, một số khía cạnh của khung bảo mật có thể và phải được tùy chỉnh để đảm bảo rằng nó phù hợp với nhu cầu của cơ quan/tổ chức. Nếu không có sự tuỳ chỉnh này, tập hợp các quy trình, thủ tục và hướng dẫn công việc sẽ trở thành gánh nặng và chi phí cho cơ quan/tổ chức sẽ bị coi là vô ích và không mang lại giá trị với việc đảm bảo an toàn.

Bất kỳ người triển khai ISO/IEC 27000 có kinh nghiệm nào sẽ cho thấy rằng phần lớn việc chuẩn bị cần thiết cho ISMS là tìm hiểu cách tổ chức hoạt động, phỏng vấn các bên liên quan và thực hiện đánh giá rủi ro. Điều này làm nổi bật mức độ chịu đựng rủi ro của người điều hành và điều chỉnh phù hợp với ngữ cảnh và và độ phức tạp của cơ quan/tổ chức.

Hình dưới đây giới thiệu tổng quan về bộ tiêu chuẩn ISO 27000.




**Hình 4-1. Bộ tiêu chuẩn ISO 27000**

*Các tiêu chuẩn về tổng quan và thuật ngữ:*

- ISO/IEC 27000:2012 – Công nghệ thông tin – Các kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin – Tổng quan và thuật ngữ.
- Tổng quan về bộ các tiêu chuẩn ISMS. Giới thiệu hệ thống quản lý an toàn thông tin. Các thuật ngữ và định nghĩa được sử dụng trong ISMS

*Các tiêu chuẩn đưa ra yêu cầu:*

- ISO/IEC 27001:2009 – Công nghệ thông tin; Các kỹ thuật an toàn;Hệ thống quản lý an toàn thông tin; Các yêu cầu bao gồm
  - Mô hình cho việc thiết lập, triển khai, vận hành, giám sát, soát xét, bảo trì và nâng cấp hệ thống quản lý an toàn thông tin.
  - Nội dung hệ thống quản lý an toàn thông tin. Trách nhiệm của cấp quản lý. Đánh giá nội bộ hệ thống ISMS. Soát xét, Cải tiến hệ thống ISMS.
- ISO/IEC 27006:2011 – Công nghệ thông tin; Các kỹ thuật an toàn; Các yêu cầu đối với các tổ chức đánh giá và cấp chứng nhận hệ thống quản lý an toàn thông tin. Tiêu chuẩn này đưa ra các yêu cầu chính thức đối với các tổ chức chứng nhận các tổ chức khác tuân thủ ISO/IEC 27001.

*Các tiêu chuẩn đưa ra hướng dẫn chung:*

- ISO/IEC 27002:2005 – Công nghệ thông tin;Các kỹ thuật an toàn; Quy tắc thực hành quản lý an toàn thông tin.
  - Thiết lập các định hướng và nguyên tắc chung cho khởi tạo, triển khai, duy trì và cải tiến công tác quản lý an toàn thông tin.
  - Gồm 134 biện pháp cho an toàn thông tin và được chia thành 11 nhóm: Chính sách, tổ chức, quản lý, nhân lực, vật lý, kiểm soát, truyền thông, xử lý sự cố….
- ISO/IEC 27003:2005 – Công nghệ thông tin; Các kỹ thuật an toàn; Hướng dẫn triển khai hệ thống quản lý an toàn thông tin. Hướng dẫn thực hành phát triển một kế hoạch triển khai hệ thống quản lý an toàn thông tin theo ISO/IEC 27001.
- ISO/IEC 27004:2009 – Công nghệ thông tin; Các kỹ thuật an toàn; Quản lý an toàn thông tin; Đo lường đánh giá**.**
  - Hướng dẫn đo lường đánh giá, báo cáo và cải thiện hiệu lực của các hệ thống ISMS một cách có hệ thống.
  - Bao gồm: tổng quan về đo lường, đánh giá; trách nhiệm; chỉ số và bài đo, triển khai đo, phân tích và báo cáo kết quả, đánh giá và cải tiến.
- ISO/IEC 27005:2008 **–** Công nghệ thông tin;Các kỹ thuật an toàn - Quản lý rủi ro an toàn thông tin.
  - Hướng dẫn quản lý rủi ro an toàn thông tin.
  - Bao gồm từ phân tích rủi ro đến việc thiết lập kế hoạch xử lý rủi ro
- ISO/IEC 27007:2011 **–** Công nghệ thông tin; Các kỹ thuật an toàn; Hướng dẫn đánh giá hệ thống quản lý an toàn thông tin.
  - Hướng dẫn cho các tổ chức cấp chứng nhận, các đánh giá viên quốc tế, các đánh giá viên bên ngoài/bên thứ ba và các đánh giá viên khác về ISMS theo ISO/IEC 27001.
  - Bao gồm: Quản lý chương trình đánh giá ISMS; Thực hiện đánh giá; Quản lý các đánh giá viên ISMS
- ISO/IEC 27008:2011 **–** Công nghệ thông tin; Các kỹ thuật an toàn; Hướng dẫn đánh giá viên đánh giá các biện pháp quản lý của hệ thống quản lý an toàn thông tin**:**
  - Hướng dẫn các đánh giá viên đánh giá các biện pháp quản lý của hệ thống quản lý AN TOÀN THÔNG TIN. hỗ trợ quy trình quản lý an toàn thông tin và các cuộc đánh giá do nội bộ, bên ngoài hoặc bên thứ ba thực hiện.

*Các tiêu chuẩn đưa ra hướng dẫn theo ngành nghề cụ thể*

- ISO/IEC 27010:2012 – Công nghệ thông tin ; Các kỹ thuật an toàn ; Quản lý an toàn thông tin cho truyền thông liên ngành và liên tổ chức hướng dẫn chia sẻ thông tin về các rủi ro AN TOÀN THÔNG TIN, các biện pháp quản lý, các vấn đề và/hoặc các sự cố xảy ra trong phạm vi giữa các ngành nghề và/hoặc các quốc gia, đặc biệt là các sự cố ảnh hưởng đến cơ sở hạ tầng quan trọng.
- ISO/IEC 27011:2008 – Công nghệ thông tin ; Các kỹ thuật an toàn : Hướng dẫn quản lý an toàn thông tin cho các tổ chức viễn thông dựa trên ISO/IEC 27002 và hướng dẫn hỗ trợ việc triển khai quản lý an toàn thông tin trong các tổ chức viễn thông.
- ISO/IEC 27015:2012 – Công nghệ thông tin ; Các kỹ thuật an toàn: Hướng dẫn quản lý an toàn thông tin cho các dịch vụ tài chính và nhấn mạnh và mở rộng một số khuyến nghị của ISO/IEC 27002 cho các tổ chức cung cấp dịch vụ tài chính.
- ISO/IEC 27799:2008 – Thông tin sức khỏe - Quản lý an toàn thông tin sức khỏe khi áp dụng ISO/IEC 27002: ***h***ướng dẫn cho các tổ chức y tế và các tổ chức nắm giữ thông tin sức khỏe cá nhân bảo vệ các thông tin sức khỏe khi triển khai ISO/IEC 27002.
- ISO/IEC 27031:2011 – Công nghệ thông tin ; Các kỹ thuật an toàn: Hướng dẫn về sự sẵn sàng của ICT để đạt được sự liên tục về nghiệp vụ và đưa ra hướng dẫn về công nghệ thông tin và truyền thông để đạt được sự liên tục về nghiệp vụ.
- ISO/IEC 27032:2012 – Công nghệ thông tin ; Các kỹ thuật an toàn ; Hướng dẫn an toàn mạng thực tại ảo và tập trung vào các khía cạnh khác nhau về an toàn trên mạng internet
- ISO/IEC 27033: 1-4 – Công nghệ thông tin ; Các kỹ thuật an toàn ; An toàn mạng. Hướng dẫn chi tiết về các khía cạnh an toàn của quản lý, vận hành, và sử dụng các mạng hệ thống thông tin và các kết nối mạng. Hướng dẫn chi tiết về triển khai các biện pháp quản lý đã được đề cập trong ISO/IEC 27002
- ISO/IEC 27034-1:2011 – Công nghệ thông tin ; Các kỹ thuật an toàn ; An toàn ứng dụng**.** Hướng dẫn an toàn thông tin cho nhân viên đặc tả, thiết kế/lập trình, triển khai và sử dụng các hệ thống ứng dụng, các nhân viên quản lý CNTT, phát triển, đánh giá và những người sử dụng đầu cuối của các hệ thống ứng dụng.
- ISO/IEC 27035: 2011– Công nghệ thông tin; Các kỹ thuật an toàn; Quản lý sự cố an toàn thông tin. Hướng dẫn các quy trình xử lý các sự cố và các điểm yếu về an toàn thông tin

## 4.3 Hệ thống tiêu chuẩn NIST

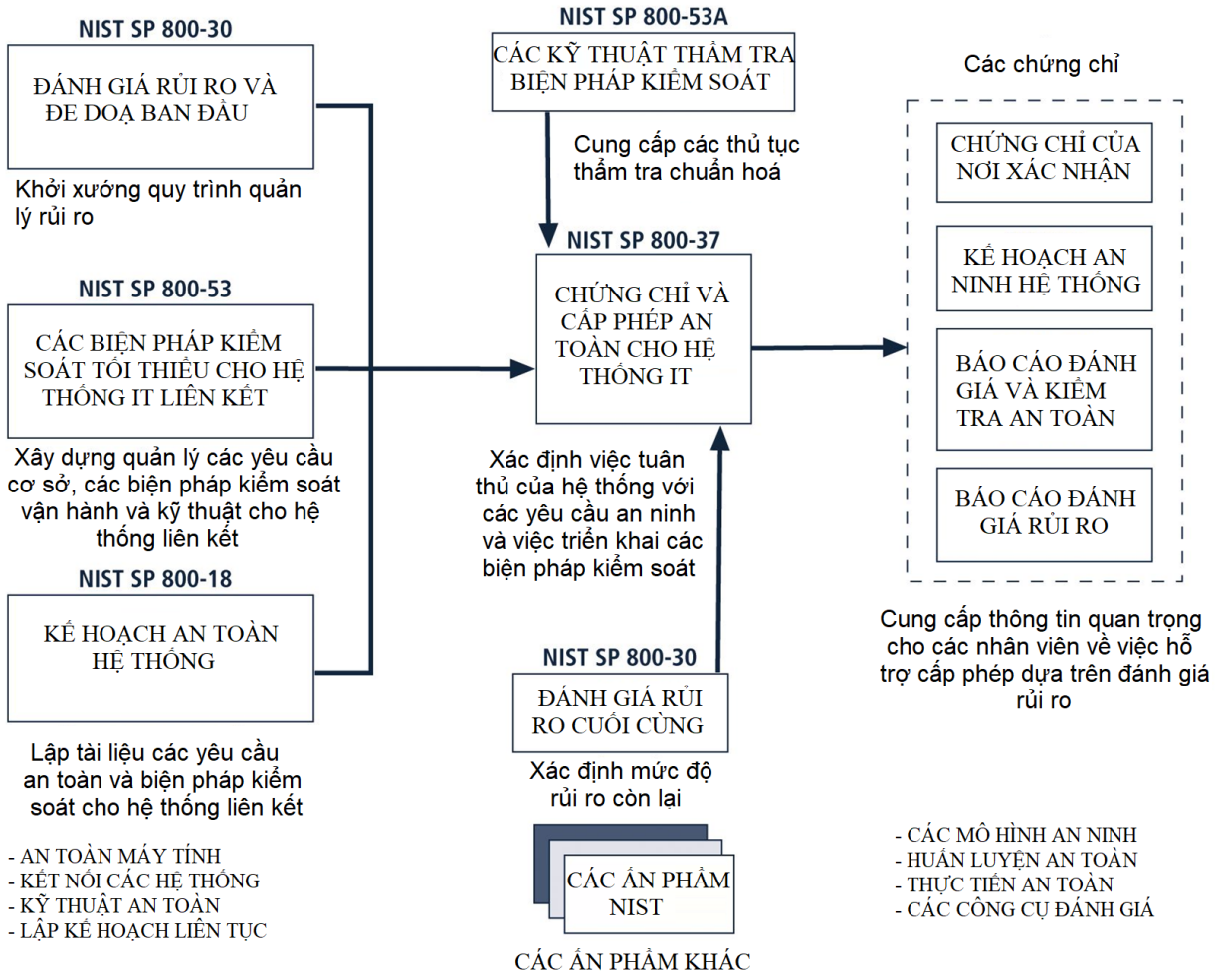
Cách tiếp cận khác về xây dựng và phát triển khung an toàn hiện có được mô tả trong các văn bản có từ trung tâm tài nguyên an toàn máy tính (*csrc.nist.gov*) với bộ tài liệu NIST 800. Bộ tài liệu NIST 800 là một tập hợp các tài liệu mô tả chính sách, thủ tục và hướng dẫn bảo mật máy tính của chính phủ liên bang Hoa Kỳ- NIST (Viện Tiêu chuẩn và Công nghệ Quốc gia). Các tài liệu có sẵn miễn phí có thể hữu ích cho các doanh nghiệp và các tổ chức giáo dục, cũng như các cơ quan chính phủ.

Các ấn phẩm trong bộ NIST 800 được phát triển như là kết quả của nghiên cứu toàn diện về các phương pháp hiệu quả và tối ưu cho an toàn hệ thống và mạng một cách chủ động. Các ấn phẩm bao gồm tất cả các quy trình và tiêu chuẩn được NIST đề xuất để đánh giá và lập tài liệu các mối đe dọa và các lỗ hổng và để thực hiện các biện pháp an toàn nhằm giảm thiểu rủi ro các sự kiện bất lợi. Các ấn phẩm có thể dùng như các hướng dẫn để thực thi các quy tắc an toàn và các tham chiếu pháp lý trong trường hợp kiện tụng liên quan đến các vấn đề an ninh.

Dưới đây là một số tài liệu tiêu biểu:

- **NIST SP 800-12** – Sổ tay an toàn máy tính
- **NIST SP 800-14** – Các nguyên tắc và quy định được chấp nhận rộng rãi để đảm bảo an toàn cho hệ thống CNTT
- **NIST SP 800-18** – Hướng dẫn phát triển khách hàng an toàn cho hệ thống CNTT-
- **NIST SP 800-37** – Hướng dẫn áp dụng khung quản lý rủi ro cho Hệ thống thông tin liên bang theo phương pháp tiếp cận vòng đời an toàn. Tài liệu này cung cấp một cách tiếp cận chi tiết gồm sáu bước để quản lý rủi ro được gọi là Khung quản lý rủi ro (RMF): phân loại, chọn, thực hiện, đánh giá, ủy quyền và giám sát.
- **NIST SP 800-53** – Đề xuất các biện pháp kiểm soát an ninh cho các hệ thống thông tin liên bang và các tổ chức và lập tài liệu các biện pháp kiểm soát an ninh cho tất cả các hệ thống thông tin liên bang, ngoại trừ các hệ thống được thiết kế cho an ninh quốc gia. NIST 800-53

Hình dưới đây biểu diễn mối tương quan giữa các tài liệu với ấn phẩm NIST SP800-53.




**Hình 4-2. Các tài liệu bổ sung NIST SP 800-37.**

## 4.4 Hệ thống tiêu chuẩn an toàn thông tin của Việt Nam

Hệ thống tiêu chuẩn an toàn thông tin của Việt Nam được xây dựng và phát triển dựa trên các tiêu chuẩn và khuyến nghị về an toàn thông tin của tổ chức ISO. Với hệ thống thông tin, hiện có 16 tiêu chuẩn về các yêu cầu, kỹ thuật an toàn, các tiêu chí đánh giá và quản lý rủi ro.

- TCVN ISO/IEC 27002:2011 Công nghệ thông tin-Các kỹ thuật an toàn- Quy tắc thực hành Quản lý an toàn thông tin
- TCVN 8709-2011 ISO/IEC 15408-2:2008 Công nghệ thông tin- Các kỹ thuật an toàn- bao gồm các yêu cầu an toàn, các tiêu chí và kỹ thuật đánh giá an toàn CNTT
- TCVN 10295:2014 ISO/IEC 27005:2011 Công nghệ thông tin-Các kỹ thuật an toàn-Quản lý rủi ro an toàn thông tin
- TCVN 10541:2014 ISO/IEC 27003:2010 Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn triển khai hệ thống quản lý an toàn thông tin

- TCVN 10543:2014 ISO/IEC 27010:2012 Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý an toàn trao đổi thông tin liên tổ chức, liên ngành
- TCVN 9801-2015 Công nghệ thông tin - Các kỹ thuật an toàn - An toàn mạng bao gồm hướng dẫn thiết kế và triển khai an toàn mạng và các kịch bản tham chiếu.
- TCVN 11239:2015 Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý sự cố an toàn thông tin
- TCVN 11386:2016 Công nghệ thông tin - Các kỹ thuật an toàn - Phương pháp đánh giá an toàn công nghệ thông tin

Hiện nay, Bộ Thông tin và Truyền thông đang gấp rút hoàn thành và chuẩn bị ban hành bổ sung các TCVN còn thiếu:

- Tiêu chuẩn hệ thống quản lý an toàn thông tin (ISO/IEC 27000:2012, ISO/IEC 27003:2010, ISO/IEC 27004:2009, ISO/IEC 27010:2012),
- Tiêu chuẩn về an toàn mạng (ISO/IEC 27033-3:2010, ISO/ IEC 27033-2:2012),
- Tiêu chuẩn về quản lý sự cố an toàn thông tin (ISO/IEC 27035:2011).

Một số TCVN khác cũng đang được tập trung xây dựng gồm có:

- Hướng dẫn bổ sung về ISMS (ISO/IEC 27006, ISO/IEC 27007, ISO/IEC 270011, ISO/ IEC 27013, ISO/IEC 27015);
- Hướng dẫn đánh giá an toàn công nghệ thông tin (ISO/IEC 18045, ISO/IEC TR 15446:2004);
- Chọn lựa, triển khai và vận hành các hệ thống phát hiện xâm nhập (ISO/IEC 18043:2006);
- An toàn sinh trắc học (ISO/IEC 19792, ISO/IEC 24761);
- Chống chối bỏ (ISO/IEC 13888)

## 4.5 Câu hỏi ôn tập

1. Nêu các ích lợi của hệ thống tiêu chuẩn an toàn thông tin mà người quản lý cần xem xét.
2. Trình bày mục tiêu của bộ tiêu chuẩn an toàn ISO 17799?
3. Nêu các điểm cần lưu ý với bộ tiêu chuẩn ISO 27000?
4. Liệt kê các tiêu chuẩn an toàn thông tin của Việt Nam đã được ban hành?
5. Giới thiệu cách thức IETF đưa ra các tiêu chuẩn của mình.
6. Giới thiệu về tổ chức ISO, NIST, ICE, IEEE.

# CHƯƠNG 5. QUẢN LÝ VẬN HÀNH KHAI THÁC AN TOÀN

Chương này trình bày các yêu cầu căn bản đối với việc vận hành và sử dụng hệ thống cũng như các nhiệm vụ đảm bảo an toàn cần thực hiện. Vấn đề về quy trình quản lý thay đổi trong cấu hình hệ thống và các cách thức kiểm soát thiết bị và dữ liệu cũng được trình bày trong chương.

## 5.1 Nguyên tắc quản lý vận hành an toàn

Vận hành an toàn liên quan đến tất cả mọi thứ diễn ra để giữ cho mạng, hệ thống máy tính, ứng dụng và môi trường và chạy theo cách thức an toàn và bảo vệ. Việc này đảm bảo rằng mọi người, ứng dụng và máy chủ có quyền truy cập thích hợp chỉ với các tài nguyên mà họ có quyền và giám sát việc thực hiện thông qua kiểm soát, kiểm toán và kiểm soát báo cáo. Các hoạt động này diễn ra sau khi hệ thống được phát triển và triển khai. Điều này bao gồm việc duy trì liên tục môi trường và các hoạt động sẽ diễn ra hàng ngày hoặc hàng tuần. Các hoạt động này lặp lại một cách thường xuyên và tự nhiên. Chúng cho phép hệ thống và các máy tính cá nhân hoạt động một cách liên tục, chính xác và an toàn.

Về cơ bản, mục tiêu của việc vận hành an toàn đảm bảo tài sản thông tin an toàn trong quá trình lưu trữ trong máy tính hay phương tiện lưu trữ khi trao đổi qua các kênh liên lạc hay trong quá trình xử lý. Bên cạnh đó, vận hành an toàn xác định các biện pháp kiểm soát phần cứng, phương tiện và người quản trị và vận hành có đặc quyền truy nhập tới các tài nguyên này.

### 5.1.1 *Nguyên tắc nhân sự*

Với các giải pháp nhằm đảm bảo an toàn cho hệ thống, yếu tố con người là vấn đề thách thức nhất. Vấn đề này càng quan trọng hơn với những người chịu trách nhiệm vận hành hệ thống. Các nguyên tắc sau đây cần được xem xét và vận dụng một cách cẩn trọng.

- Đặc quyền tối thiểu hay biết những thứ cần thiết (*need-to-know*)
  - Chỉ được phép truy nhập thông tin cần để hoàn thành công việc - Giữ bí mật thông tin
  - Chỉ cấp quyền tối thiểu để thực hiện công việc – Giữ tính toàn vẹn thông tin
- Tách biệt chức vụ và trách nhiệm
  - Không người dùng nào có toàn quyền kiểm soát hệ thống – không ai có thể làm tổn hại hệ thống hay các biện pháp kiểm soát

- Tạo ra hệ thống kiểm soát và đối trọng (checks-and-balances): luôn có người dùng giám sát và kiểm tra công việc lẫn nhau
- Chia tách công việc/chức vụ: đảm bảo không ai lạm dụng truy nhập hệ thống có thể gây là việc xung đột lợi ích hay che dấu hành vi xâm phạm hệ thống
- Phân chia các quyền để thực hiện công việc

▪ Giám sát các đặc quyền
- Các hoạt động sử dụng đặc quyền thực hiện các công việc quản trị hay nhiệm vụ nhạy cảm như tạo người dùng, thay đổi cấu hình hệ thống
- Đảm bảo các quyền này không bị lạm dụng

• An toàn cho cán bộ/nhân viên
- Cán bộ và nhân viên là tài sản quan trọng nên cần đảm bảo môi trường làm việc an toàn và hạn chế rủi ro về thể chất và tinh thần đặc biệt những người phụ trách vấn đề an toàn.

▪ Tính giải trình
- Việc truy nhập và sử dụng tài nguyên của hệ thống cần được giám sát, kiểm toán và ghi nhật ký một cách thích đáng
- Cần đảm bảo người dùng truy nhập và sử dụng tài nguyên một cách phù hợp với yêu cầu công việc

### 5.1.2 *Nhiệm vụ vận hành an toàn*

Việc vận hành an toàn nhấn mạnh biện pháp đảm bảo an toàn và đối phó để bảo vệ các tài nguyên thông tin, các phần cứng hỗ trợ. Mục tiêu của việc vận hành an toàn là giảm thiểu tổn hại có thể xảy ra do truy nhập trái phép hay lộ bí mật bằng cách hạn chế việc lỡ làm sai hay lạm dụng.

Các hoạt động trong môi trường điện toán có thể liên quan đến phần mềm, nhân sự và phần cứng, nhưng bộ phận vận hành thường tập trung vào các khía cạnh phần cứng và phần mềm. Những người vận hành chịu trách nhiệm đảm bảo rằng các hệ thống được bảo vệ và hoạt động một cách liên tục theo cách có thể dự đoán được.

Bộ phận vận hành thường có mục tiêu ngăn ngừa các vấn đề định kỳ, giảm hư hỏng phần cứng và phần mềm xuống mức chấp nhận được và giảm tác động của sự cố hoặc gián đoạn. Bộ phận này cần điều tra bất kỳ sự cố bất thường hoặc không rõ nguyên nhân, nạp các chương trình khởi động bất thường, lệch chuẩn hoặc các điều kiện kỳ lạ hoặc bất thường khác diễn ra trên hệ thống.

Các nhiệm vụ của người vận hành cơ bản ứng phó khi sự việc diễn ra:

- *Tình huống bất thường*. Do mạng, phần cứng và các phần mềm phức tạp và biến động nên khi có tình huống xảy ra khó giải thích. Vì vậy người quản trị cần thực hiện việc điều tra, chuẩn đoán và đưa ra giải pháp lô-gíc.
- *Lệch chuẩn*. Mỗi phần mềm, phần cứng có các tiêu chuẩn nhất định: thời gian hoạt động, số các yêu cầu có thể xử lý,... Đây là cơ sở để xác định liệu có vấn đề với phần cứng hay phần mềm
- *Khởi động chương trình bất thường*. Chương trình khởi động là thuật ngữ mô tả việc nạp hệ điều hành vào bộ nhớ chính. Người quản trị cần điều tra các máy tính khởi động bất thường để xác định nguyên nhân và rủi ro tiềm tàng
- *Xác định và quản lý tài sản*. Nắm bắt thông tin chi tiết về các tài sản của cơ quan/tổ chức. Điều kiện tiên quyết để biết liệu phần cứng (bao gồm cả hệ thống và mạng) và phần mềm có trong cấu hình an toàn hay không là biết phần cứng và phần mềm nào hiện diện trong môi trường hoạt động. Quản lý tài sản bao gồm việc biết và cập nhật phần cứng (hệ thống và mạng) và phần mềm hiện đang có.
- *Kiểm soát hệ thống*. Đây cũng là một phần của vận hành an toàn. Trong chính bản thân hệ điều hành, các kiểm soát nhất định phải được đặt ra để đảm bảo rằng các lệnh được thực hiện trong ngữ cảnh bảo mật chính xác. Hệ thống có các cơ chế hạn chế việc thực hiện một số loại lệnh nhất định để chúng chỉ có thể diễn ra khi hệ điều hành ở trạng thái đặc quyền hoặc giám sát. Điều này bảo vệ an ninh tổng thể và trạng thái của hệ thống và giúp đảm bảo hệ thống chạy một cách ổn định và theo cách có thể dự đoán được.

  Các thủ tục vận hành cần phải được phát triển để xác định các cấu thành của việc vận hành đúng đắn của hệ thống hoặc tài nguyên. Việc này sẽ bao gồm việc khởi động hệ thống và quy trình tắt, xử lý lỗi, và khôi phục từ nguồn tin cậy.
- *Khôi phục tin cậy*. Khi có lỗi với hệ điều hành thì có thể được phân loại thành: Khởi động lại, khởi động hệ thống ở chế độ khẩn cấp, khởi động nguội. Khi hệ điều hành hay ứng dụng bị treo hay hỏng, phải không để cho hệ thống rơi vào trạng thái mất an toàn khi phục hồi hệ thống.

  Việc *khởi động lại* hệ thống diễn ra sau khi hệ thống tự tắt theo cách được điều khiển để xử lý lỗi phần nhân (cơ sở tính toán tin cậy). Nếu hệ thống thấy tồn tại các dữ liệu không nhất quán hoặc nếu không có đủ bộ nhớ, việc khởi động lại hệ thống có thể diễn ra. Điều này giải phóng tài nguyên và trả về hệ thống về trạng thái ổn định và an toàn hơn.

  Khởi động lại hệ thống khẩn cấp diễn ra sau khi xảy ra lỗi hệ thống theo cách không kiểm soát được. Đây có thể là lỗi phần nhân hoặc lỗi do các chương trình người dùng có đặc quyền thấp hơn cố gắng truy cập vào các phần bộ nhớ bị hạn chế. Hệ thống coi đây là một hoạt động không an toàn mà nó không thể

phục hồi đúng cách mà không cần khởi động lại. Phần nhân và chương trình người dùng có thể ở trạng thái không nhất quán và dữ liệu có thể bị mất hoặc bị hỏng. Do đó, hệ thống sẽ chuyển sang chế độ bảo trì và khôi phục từ các hành động đã thực hiện. Sau đó, hệ thống được đưa trở lại trong trạng thái nhất quán và ổn định.

Hệ thống khởi động nguội xảy ra khi phần nhân bị lỗi bất ngờ hoặc bộ nhớ hỏng và các thủ tục khôi phục thông thường không thể phục hồi hệ thống đến trạng thái nhất quán hơn. Các phần mềm hệ thống, nhân và người dùng có thể vẫn ở trạng thái không nhất quán trong khi hệ thống cố gắng khôi phục chính nó và người dùng hoặc quản trị viên có thể yêu cầu can thiệp để khôi phục hệ thống.

Sau khi hệ thống bị hỏng cần:

- Chuyển sang chế độ 1 người dùng hay chế độ an toàn
- Sửa lỗi và khôi phục file
- Kiểm tra các file và các hoạt động quan trọng

Vấn đề an toàn: Khi hệ điều hành ở tình huống không ổn định thì luôn phải xem xét có lỗ hổng kiểu nào đó đang tồn tại bao gồm việc xem xét và thực hiện:

- Trình tự khởi động
- Ghi nhật ký hệ thống phải được thực hiện đầy đủ
- Việc tắt cưỡng bức hệ thống không được phép
- Đầu ra dữ liệu không được phép chuyển hướng

- *Kiểm soát dữ liệu vào/ra.* Đầu vào của ứng dụng có mối tương quan trực tiếp với kết quả mà ứng dụng xuất ra. Do đó, đầu vào cần được giám sát lỗi và hoạt động đáng ngờ. Bản thân các ứng dụng cũng cần phải được lập trình để chỉ chấp nhận một số dạng giá trị đầu vào vào chúng và thực hiện các kiểm tra logic về các giá trị đầu vào nhận được.

  Tất cả các cơ chế kiểm soát được đề cập trong các phần trước phải được đặt ra và phải tiếp tục hoạt động trong một thời trang có thể dự đoán và an toàn để đảm bảo rằng các hệ thống, ứng dụng và môi trường nói chung tiếp tục hoạt động. Một số vấn đề khác có thể gây ra sự cố nếu không được xử lý đúng cách:

  - Dữ liệu vào phải được giám sát để phát hiện lỗi hay hành vi bất thường
  - Dữ liệu vào phải được kiểm tra để tránh lỗi cho chương trình
  - Dữ liệu đầu ra phải được lưu lại và đóng dấu thời gian

- *Tăng cường an ninh.* Một chủ đề lặp lại trong bảo mật là các biện pháp kiểm soát thường được mô tả là vật lý, hành chính hoặc kỹ thuật. Điều đáng chú ý rằng nếu truy cập vật lý trái phép có thể tiếp cận tới phần tử nhạy cảm an ninh,

thì việc bảo mật cho phần tử này là hầu như không thể đảm bảo. Rõ ràng, chính trung tâm dữ liệu phải được bảo vệ về mặt vật lý. Điều này tạo ra một vành đai an ninh chặt chẽ quanh các cơ sở nơi lưu trữ thông tin có giá trị.

Trong mô hình lý tưởng, các ứng dụng và phương thức truy nhập thông tin sẽ được bảo vệ chống lại bất kỳ cuộc tấn công mạng nào; tuy nhiên, thực tế không lý tưởng và trách nhiệm của chuyên gia an ninh là bảo mật thông tin có giá trị trong thế giới thực. Do đó, các thành phần vật lý tạo nên các mạng thông qua đó các luồng thông tin có giá trị cũng phải được bảo đảm:

- Khóa tủ đấu dây, tủ Hub, chuyển mạch mạng
- Các cổng kết nối cần phải cấm truy nhập
- Chỉ sử dụng phần mềm tối thiểu

- *An toàn truy nhập từ xa.* Là phần quan trọng trong việc vận hành bình thường của hệ thống, giúp giảm chi phí và tăng hiệu quả làm việc cho nhân viên. Tuy nhiên, việc này phức tạp trong việc kiểm soát an toàn bao gồm: xác thực người dùng, bảo mật đường truyền. Vì vậy cần hạn chế/xác định rõ người dùng được phép sử dụng dịch vụ này. Một số vấn đề cần chú ý để đảm bảo lợi ích của việc truy nhập từ xa:
  - Các lệnh và dữ liệu không nên được thực hiện dưới dạng văn bản rõ. Ví dụ, Secure Shell (SSH) nên được sử dụng chứ không phải telnet.
  - Các hệ thống thực sự quan trọng nên được quản lý cục bộ thay vì từ xa.
  - Chỉ một số ít người quản trị có thể thực hiện chức năng từ xa này.
  - Cần thực hiện xác thực mạnh cho bất kỳ hoạt động quản trị nào.
  - Người dùng khả nghi không được truy cập vào các hệ thống này.

### 5.1.3 *Các độ do cơ bản*

Dưới đây làm một số số đo cơ bản đánh giá khả năng hoạt động của các thiết bị trong hệ thống máy tính và mạng. Các số đo này giúp người quản lý hình dung được các điểm yếu cũng như chi phí cho việc đảm bảo vận hành an toàn của thiết bị cũng như hệ thống.

a. *Thời gian trung bình giữa các lỗi (MTBF)*

MTBF *(Mean Time Between Failures*) là tuổi thọ ước tính của một thiết bị và được tính bởi nhà cung cấp thiết bị hoặc bên thứ ba. Giá trị này cho biết biết khoảng thời gian một thiết bị cụ thể sẽ cần phải được thay thế. Giá trị MTBF được sử dụng như một tiêu chuẩn về độ tin cậy bằng cách ước lượng thời gian trung bình của thiết bị hoặc một hệ thống từ lúc hoạt động cho đến khi hỏng hẳn (hay chết) dựa trên dữ liệu lịch sử hoặc được các nhà cung cấp ước tính một cách khoa học. Các cơ quan/tổ chức thường sử dụng MTBF để có thể xác định các loại thiết bị không vượt quá mức sử dụng trung bình do nhà sản xuất cam kết và chủ động liên hệ với nhà sản xuất theo bảo hành hoặc quyết định

rằng thiết bị đang đến điểm cuối của việc vận hành hữu ích và chọn để thay thế thiết bị đó trước khi xảy ra sự cố quy mô lớn hơn và làm gián đoạn hoạt động của cơ quan/tổ chức.

b. *Thời gian trung bình để sửa chữa (MTTR)*

MTTR (*Mean Time To Repair*) là khoảng thời gian cần thiết để thiết bị được sửa chữa và quay trở lại hoạt động. Đối với một ổ đĩa cứng trong chuỗi ổ cứng dự phòng, MTTR là khoảng thời gian giữa sự cố thực tế và thời gian khi, sau khi nhận thấy lỗi, người ta thay thế ổ đĩa bị lỗi và chuỗi ổ cứng dự phòng hoàn thành ghi lại thông tin trên ổ đĩa mới. Điều này có thể được đo bằng giờ. Đối với ổ đĩa cứng không dự phòng trong máy tính để bàn, MTTR là khoảng thời gian giữa khi người dùng phát ra lỗi lớn, yêu cầu trợ giúp và thời gian ổ đĩa cứng thay thế được nạp lại với hệ điều hành, phần mềm và mọi dữ liệu được sao lưu thuộc về người dùng. Điều này có thể được đo bằng ngày.

Với khởi động lại không lập kế hoạch, MTTR là khoảng thời gian giữa sự sự cố của hệ thống và thời điểm khi hệ thống này khởi động lại hệ điều hành, kiểm tra trạng thái đĩa, và khởi động lại các ứng dụng, và các ứng dụng của hệ thống đã kiểm tra tính nhất quán của dữ liệu và một lần nữa bắt đầu xử lý các giao dịch. Đối với phần cứng được xây dựng tốt chạy phần mềm và hệ điều hành có chất lượng cao, được quản lý tốt, điều này có thể chỉ mất vài phút. Đối với tình huống không có hệ thống và cơ sở dữ liệu hiệu năng cao, điều này có thể là hàng giờ, hoặc tệ hơn, hàng ngày nếu khôi phục không hoạt động và cần khôi phục dữ liệu từ thiết bị lưu trữ:

- MTTR có thể liên quan đến việc sửa chữa thành phần hoặc thiết bị hoặc thay thế thiết bị.
- Nếu MTTR quá cao đối với thiết bị quan trọng, thì nên sử dụng dự phòng.

Số MTBF và MTTR do nhà sản xuất cung cấp rất hữu ích trong việc chọn chi phí cho các hệ thống mới. Các hệ thống có thể bị dừng trong một thời gian ngắn mà không có ảnh hưởng đáng kể có thể được xây dựng từ các thành phần không tốn kém với kỳ vọng MTBF thấp hơn và MTTR khiêm tốn. Giá trị MTBF cao hơn thường đi kèm với chi phí lớn hơn. Các hệ thống không thể được dừng cần các thành phần dự phòng. Hệ thống không cho phép dừng khi một thành phần dự phòng đã hỏng và đang được thay thế có thể cần khả năng chịu lỗi.

c. *Điểm nghẽn*

SPOF (*Single Point Of Failure*) là lỗi gây ra nhiều rủi ro tiềm ẩn cho một mạng hay hệ thống. Khi thiết bị mạng bị lỗi, một phân đoạn hoặc thậm chí toàn bộ mạng bị ảnh hưởng tiêu cực. Các thiết bị tiêu biểu cho điểm nghẽn như tường lửa, bộ định tuyến, máy chủ truy cập mạng hay máy chủ xác thực. Cách tốt nhất chống lại việc tổn thương bởi các điểm nghẽn này là bảo trì thích đáng, sao lưu thường xuyên, dự phòng và khả năng chịu lỗi.

Ổ đĩa dự phòng độc lập RAID cung cấp khả năng chịu lỗi cho việc lưu trữ dữ liệu và cải thiện hiệu năng hệ thống. Dự phòng và hiệu năng được đảm bảo bằng cách chia nhỏ dữ liệu và ghi chúng trên nhiều đĩa để các đĩa khác nhau có thể làm việc đồng thời với yêu cầu truy xuất thông tin. Dữ liệu kiểm soát cũng được phân tán trên mỗi đĩa như là mã chẵn lẻ để nếu một đĩa bị hỏng các đĩa khác có thể làm việc cùng nhau và khôi phục dữ liệu.

## 5.2 Quản lý cấu hình

Mọi cơ quan/tổ chức nên có chính sách chỉ ra cách thay đổi diễn ra trong một bộ phận:

- Làm thế nào để các thay đổi với các phương tiện/thiết bị được thực hiện
- Ai là người thực hiện
- Cách thức phê chuẩn sự thay đổi
- Cách thức lập tài liệu và thông báo về sự thay đổi với các cán bộ/nhân viên khác

Nếu không có những chính sách này, mọi người có thể thực hiện những thay đổi mà người khác không biết, không được chấp thuận, điều này có thể dẫn đến một mớ hỗn độn khó hiểu ở mức thấp nhất và hư hỏng hoàn toàn các hoạt động ở mức cao. Các ngành có các quy định chặt chẽ như ngân hàng, tài chính, viễn thông, và năng lượng có những hướng dẫn rất nghiêm ngặt cụ thể về những gì có thể được thực hiện và chính xác vào thời điểm nào và trong điều kiện nào. Nếu không có các kiểm soát và hướng dẫn nghiêm ngặt, lỗ hổng vận hành có thể được đưa vào môi trường hoạt động. Theo dõi và đảo ngược các thay đổi sau khi mọi thứ được thực hiện có thể là một nhiệm vụ rất phức tạp và gần như không thể.

Những thay đổi có thể xảy ra với cấu hình mạng, thông số hệ thống, ứng dụng và cài đặt khi thêm công nghệ, cấu hình ứng dụng hoặc thiết bị mới hoặc khi sửa đổi môi trường hệ thống của cơ quan/tổ chức. Kiểm soát thay đổi quan trọng không chỉ đối với môi trường hoạt động mà còn cho một sản phẩm, như phần mềm, trong quá trình phát triển và vòng đời của nó. Các thay đổi phải hiệu quả và có trật tự bởi vì thời gian và tiền bạc có thể bị lãng phí khi liên tục thực hiện các thay đổi không đáp ứng được mục tiêu cuối cùng.

### 5.2.1 *Quy trình kiểm soát thay đổi*

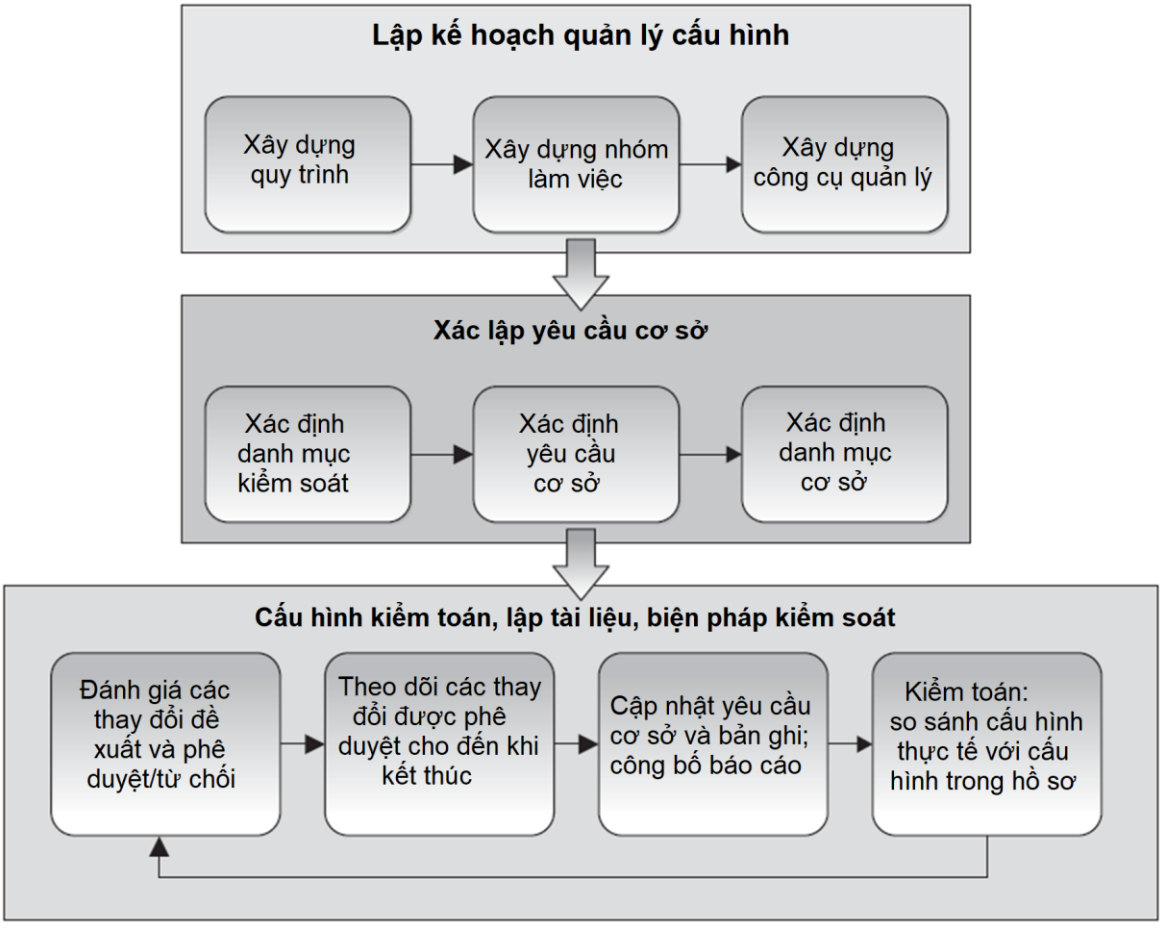
Các dạng sửa đổi hay điều chỉnh có thể khác nhau song danh mục tiêu chuẩn các thủ tục cần thực hiện giúp cho việc thay đổi được kiểm soát và đảm bảo việc thực hiện diễn ra theo cách kiểm soát được.

Các bước cơ bản của chính sách kiểm soát thay đổi:

1. *Yêu cầu thay đổi*. Yêu cầu này cần phải được gửi cho cá nhân/nhóm chịu trách nhiệm phê chuẩn sự thay đổi và giám sát các hoạt động thực hiện thay đổi

2. *Phê chuẩn sự thay đổi*. Cá nhân yêu cầu thay đổi phải giải trình lý do cũng như lợi ích và bất lợi của việc thay đổi.
3. *Lập tài liệu*. Ngay sau khi việc thay đổi được chấp thuận, việc này cần được lưu vào nhật ký (log) thay đổi
4. *Kiểm tra*. Việc thay đổi cần phải được kiểm tra đầy đủ để phát hiện kết quả chưa được dự đoán. Tùy thuộc theo mức độ trầm trọng mà thay đổi và việc triển khai phải được giải trình.
5. *Triển khai*. Sau khi việc thay đổi được chấp thuận và kiểm tra đầy đủ, kế hoạch thực hiện được xây dựng để phác thảo ra các giai đoạn thực thi cũng như các mốc quan trọng. Tất cả các bước này cần được lập tài liệu đầy đủ và tiến độ phải được giám sát.
6. *Báo cáo*. Báo cáo về sự thay đổi cần được nộp cho ban quản lý theo định kỳ

Hình vẽ dưới đây minh họa các giai đoạn trong việc quản lý cấu hình.




**Hình 5-1. Các giai đoạn quản lý cấu hình**

### 5.2.2 *Lập tài liệu về thay đổi*

Thiếu sót trong việc lập tài liệu về thay đổi hệ thống và mạng luôn tiềm ẩn rủi ro về an toàn. Không ai nhớ được bộ định tuyến đã được sửa chữa và cập nhật cái gì kể từ 6 tháng trước đó. Cấu hình hệ thống thay đổi thường xuyên nên luôn cần có nhân lực để

thực hiện việc lập tài liệu này. Các thay đổi thường xuất hiện trong quá trình hoạt động như:

- Cài đặt máy tính mới
- Cài đặt phần mềm mới
- Cấu hình mới triển khai
- Cài đặt cập nhật và bản vá
- Tích hợp công nghệ mới
- Chính sách, thủ tục và tiêu chuẩn được cập nhật
- Yêu cầu và quy định mới được triển khai
- Vấn đề mạng hay hệ thống được xác định và sửa chữa
- Cấu hình mạng khác được thiết lập
- Thiết bị mạng mới được tích hợp vào trong mạng

## 5.3 Kiểm soát thiết bị, dữ liệu

Các phương tiện và thiết bị lưu trữ được sử dụng rộng rãi trong quá trình vận hành của hệ thống và cần nhiều biện pháp kiểm soát để đảm bảo chúng được duy trì thích đáng và tính toàn vẹn, bí mật và sẵn sàng của dữ liệu lưu để chúng không bị xâm phạm. Các phương tiện lưu trữ có thể bao gồm các thiết bị điện tử như CD/DVD, ổ flash, ổ cứng... cũng như không phải điện tử như tài liệu in.

Các biện pháp kiểm soát tới các phương tiện lưu trữ này cũng rất đa dạng bao gồm

- Kiểm soát truy nhập trái phép: thường là kiểm soát vật lý, quản trị (chính sách), kỹ thuật
- Hạn chế truy nhập như phòng lưu trữ cần có khóa cho phép người có trách nhiệm truy cập

Bên cạnh đó, các phương tiện lưu trữ cần được đánh dấu, ghi nhật ký rõ ràng và phải được hủy một cách phù hợp khi không sử dụng nữa, ví dụ như khi thay thế hay nâng cấp ổ cứng. Việc không tuân thủ các quy định về loại bỏ các phương tiện có thể dẫn đến việc rò rỉ thông tin nằm trên các thiết bị hay phương tiện cũ.

### 5.3.1 *Xóa dữ liệu an toàn*

Khi phương tiện lưu trữ bị xóa thì nó được coi là đã thanh lọc. Điều này có nghĩa là xóa thông tin để không dễ dàng truy xuất bằng các lệnh của hệ điều hành thông thường hoặc phần mềm khôi phục dữ liệu. Việc xóa được chấp nhận khi phương tiện lưu trữ sẽ được tái sử dụng trong cùng môi trường vật lý cho cùng mục đích (trong cùng một không gian bảo mật thông tin) bởi những người có cùng mức truy cập.

Việc thanh lọc có nghĩa là làm cho thông tin không thể phục hồi ngay cả với những nỗ lực đặc biệt như các kỹ thuật điều tra số. Thanh lọc là cần thiết khi phương tiện lưu

trữ được loại bỏ khỏi không gian vật lý, nơi các thông tin trên các phương tiện lưu trữ được phép truy cập, hoặc sẽ được chuyển đến không gian khác. Phương tiện lưu trữ có thể được thanh lọc bằng nhiều cách: xóa về không (ghi đè theo mẫu được thiết kế để đảm bảo dữ liệu trước đây trên phương tiện không khôi phục được), khử từ (xáo trộn từ các mẫu trên băng hoặc đĩa đại diện cho thông tin được lưu trữ ở đó), và phá hủy (băm nhỏ, nghiền, cháy).

Xóa các tập tin trên một phần của phương tiện truyền thông không thực sự làm cho dữ liệu biến mất; nó chỉ xóa các con trỏ đến nơi dữ liệu trong các tệp đó vẫn còn tồn tại trên phương tiện. Và nếu bất kỳ phần nào của phương tiện lưu trữ chứa thông tin nhạy cảm cao không thể bị xóa hoặc bị thanh lọc, thì cần phải phá hủy vật lý phương tiện đó.

### 5.3.2 *Quản lý phương tiện lưu trữ và thiết bị*

Việc giám sát và theo dõi các phương tiện lưu trữ và thiết bị cần thực hiện các yêu cầu và nhiệm vụ căn bản như sau:

- *Theo dõi* (ghi nhật ký): lập bản ghi tại bất cứ thời điểm nào. Việc này cho phép điều tra xác định thông tin ở bất kỳ thời điểm nào, ai có thông tin nhạy cảm, và tại sao họ truy cập thông tin đó. Điều này cho phép người điều tra tập trung nỗ lực vào những người, địa điểm và thời gian cụ thể trong trường hợp nghi ngờ có lỗ hổng hoặc lỗ hổng đã xảy ra.
- *Triển khai biện pháp kiểm soát truy nhập hiệu quả*: nhằm xác định người sở hữu phương tiện lưu trữ để lựa chọn biện pháp kiểm soát phù hợp. Một số phương tiện, do tính chất vật lý và/hoặc bản chất của thông tin trên đó, có thể yêu cầu "xử lý đặc biệt". Tất cả nhân viên được phép truy cập phương tiện lưu trữ đều phải có đào tạo để đảm bảo họ hiểu những gì được yêu cầu của phương tiện đó. Ví dụ về xử lý đặc biệt cho thông tin được phân loại có thể là phương tiện lưu trữ chỉ có thể bị xóa khỏi dưới sự giám sát trực tiếp.

  Việc kiểm soát truy cập sẽ bao gồm biện pháp vật lý (cửa bị khóa, tủ hoặc két), biện pháp kỹ thuật (kiểm soát truy cập và ủy quyền của bất kỳ hệ thống tự động nào để truy xuất nội dung thông tin) và quản trị (quy tắc thực tế cho ai phải làm gì cho từng phần thông tin). Cuối cùng, dữ liệu có thể cần thay đổi định dạng, như in dữ liệu điện tử sang giấy. Dữ liệu vẫn cần phải được bảo vệ ở mức cần thiết, bất kể định dạng của nó là gì.
- *Theo dõi số và vị trí phiên bản dự phòng*. Việc này cần thiết để đảm bảo xử lý đúng thông tin khi thông tin đến hết tuổi thọ, để xác định vị trí và khả năng truy cập thông tin trong quá trình kiểm tra và tìm bản sao lưu thông tin nếu nguồn thông tin chính bị mất hoặc bị hỏng.
- *Lập tài liệu về quá trình thay đổi các phương tiện lưu trữ*: khi một phiên bản cụ thể của một ứng dụng phần mềm được lưu giữ được coi là lỗi thời, điều này phải được ghi lại để phiên bản này của ứng dụng không được sử dụng trừ khi bắt buộc. Ngay cả các phương tiện lưu trữ hoặc nội dung của nó không

còn cần thiết, việc giữ lại bản ghi về sự tồn tại của chúng và thời gian và cách thức loại bỏ nó có thể hữu ích để thể hiện sự cẩn trọng.

- *Đảm bảo điều kiện hoạt động không gây nguy hiểm phương tiện và thiết bị*. Mỗi loại phương tiện lưu trữ có thể dễ bị tổn thương do một hoặc nhiều ảnh hưởng từ môi trường. Chẳng hạn, tất cả các dạng phương tiện lưu trữ đều dễ bị cháy, và hầu hết đều dễ bị biến đổi bởi chất lỏng, khói và bụi. Các định dạng phương tiện từ tính dễ bị từ trường mạnh. Các định dạng phương tiện từ và quang học dễ bị biến đổi về nhiệt độ và độ ẩm. Các phương tiện lưu trữ cần được đảm bảo các thông số môi trường cho việc cất giữ và môi trường phải được giám sát để đảm bảo điều kiện không nằm ngoài các thông số đó.
- *Đảm bảo tính toàn vẹn cho phương tiện lưu trữ* bằng cách xác minh trên cơ sở dạng phương tiện và môi trường phù hợp cho các phương tiện lưu trữ này có thể sử dụng được. Mỗi loại phương tiện lưu trữ đều có tuổi thọ dự kiến trong một số điều kiện nhất định, sau đó nó không còn có thể đảm bảo việc lưu thông tin một cách đáng tin cậy. Ví dụ, đĩa CD hoặc DVD được sản xuất thương mại trong điều kiện môi trường tốt sẽ đáng tin cậy trong ít nhất mười năm, trong khi đĩa CD-R hoặc DVD-R rẻ tiền để trong phòng làm việc có thể trở nên không đáng tin cậy chỉ sau một năm.

  Ngoài ra, như là một phần của việc duy trì tính toàn vẹn của nội dung cụ thể của một phương tiện lưu trữ, nếu thông tin có giá trị cao hoặc bắt buộc phải được lưu giữ theo quy định luật pháp thì có thể duy trì chữ ký mã hóa nội dung của phương tiện.
- *Thực hiện các hoạt động loại bỏ an toàn.* Việc thực hiện bao gồm cả thời gian mà sau đó thông tin không còn giá trị và các biện pháp cần thiết để xử lý các phương tiện lưu trữ/ thông tin. Việc xử lý một cách an toàn các phương tiện lưu trữ/thông tin có thể làm tăng chi phí một cách đáng kể cho việc quản lý. Việc xử lý an toàn có thể làm giảm khả năng khi một phần của phương tiện lưu trữ bị ném vào thùng rác và sau đó được tìm thấy bởi ai đó và công bố công khai. Cơ quan/tổ chức phải tính đến thời gian hữu ích của thông tin đối với các yêu cầu về kinh doanh và quy định pháp lý. Nếu pháp luật hay quy định yêu cầu thông tin được lưu giữ vượt quá thời gian hoạt động bình thường của cơ quan/tổ chức thì việc loại bỏ an toàn có thể liên quan đến việc di chuyển thông tin từ khả năng truy cập sẵn sàng (và có thể tốn kém hơn) sang dạng lâu dài có thể truy xuất với chi phí lưu trữ thấp hơn.
- *Lập nhãn cho phương tiện*: ngày tháng tạo lập, mức phân loại, ngày cần hủy,...

### 5.3.3 *Tính sẵn dùng mạng và các tài nguyên*

Tính sẵn dùng là một trong các tiêu chí cơ bản cho an toàn thông tin trong các yêu cầu cơ bản của an toàn (bí mật, toàn vẹn và sẵn dùng). Mọi người thường không quan

tâm đến mạng và tài nguyên cho đến khi hệ thống bị sự cố. Vì vậy, người quản trị cần triển khai việc sao lưu và dự phòng để khi có sự cố, năng suất làm việc của hệ thống không bị ảnh hưởng nghiêm trọng. Các kỹ thuật đáng chú ý như sau:

- Phần cứng dự phòng: sử dụng kỹ thuật "thay nóng" cho phép loại bỏ phần cứng bị trục trặc và thay bằng phần cứng mới.
- Các công nghệ chịu lỗi: cho phép hệ thống vẫn hoạt động ở mức chấp nhận được khi có sự cố
- Thỏa thuận về cấp độ dịch vụ: xác định giới hạn về dịch vụ và ngân sách cho việc triển khai dịch vụ.
- Thủ tục vận hành tin cậy: xây dựng, huấn luyện và đào tạo nhân viên về việc vận hành hệ thống.

a. *Lập nhóm:*

Lập nhóm (*Clustering*) là một công nghệ máy chủ chịu lỗi tương tự như các máy chủ dự phòng, ngoại trừ mỗi máy chủ tham gia vào các dịch vụ xử lý được yêu cầu. Một cụm máy chủ là một nhóm các máy chủ được xem như một máy chủ cho người dùng và có thể được quản lý như một hệ thống logic duy nhất. Kỹ thuật này đảm bảo tính sẵn dùng và khả năng mở rộng bằng việc nhóm các hệ thống vật lý khác nhau và kết hợp chúng một cách hợp lý cung cấp khả năng miễn nhiễm các lỗi và cải thiện hiệu suất. Các cụm hoạt động như một đơn vị thông minh để cân bằng lưu lượng truy cập và người dùng truy cập cụm không biết họ có thể truy cập các hệ thống khác nhau vào các thời điểm khác nhau. Đối với người dùng, tất cả các máy chủ trong cụm được xem là một đơn vị. Các cụm cũng có thể được gọi là các trang trại máy chủ (*server farm*).

Nếu một trong các hệ thống trong cụm bị trục trặc, việc xử lý tiếp tục vì phần còn lại tiếp nhận tải mặc dù việc suy giảm hiệu năng có thể xảy ra. Tuy nhiên, điều này hấp dẫn hơn là có một máy chủ phụ (dư thừa) chờ đợi trong trường hợp máy chủ chính bị lỗi. Rõ ràng, máy chủ phụ này có thể không hoạt động trong một thời gian dài gây lãng phí. Khi phân cụm được truy nhập, tất cả các hệ thống được sử dụng để xử lý các yêu cầu và không có hệ thống nào nằm ở trạng thái sự cố.

b. *Tính toán lưới*

Tính toán lưới là một dạng cân bằng tải song song của tính toán lớn, tương tự như lập các cụm, nhưng được triển khai với các hệ thống liên kết một cách lỏng lẻo mà có thể tham gia và rời khỏi lưới một cách ngẫu nhiên. Hầu hết các máy tính không sử dụng hết năng lực của bộ xử lý nhiều quãng thời gian trong ngày. Vì vậy, người ta đưa ra một giải pháp thông minh để sử dụng tất cả sức mạnh xử lý dôi dư này. Cũng giống như lưới điện cung cấp điện cho các cơ quan trên cơ sở nhu cầu, máy tính có thể tự nguyện để cho phép các nhóm khác nhau tận dụng sức mạnh xử lý dư thừa cho các dự án khác nhau. Dự án đầu tiên sử dụng điện toán lưới là SETI (Tìm kiếm trí thông minh ngoài trái đất), nơi mọi

người cho phép các hệ thống của họ tham gia quét vũ trụ tìm người ngoài hành tinh đang cố gắng nói chuyện với con người.

Mặc dù điều này có vẻ tương tự như kỹ thuật lập nhóm, trong nhóm có một bộ điều khiển trung tâm có quyền điều khiển tổng thể phân bổ tài nguyên và người dùng cho các nút (máy chủ) trong nhóm và các nút trong nhóm nằm dưới quyền quản lý trung tâm (trong cùng một miền tin cậy). Trong lưới tính toán, các nút không tin tưởng nhau và không có quyền kiểm soát trung tâm.

Các ứng dụng có thể thích hợp về mặt kỹ thuật để chạy trong lưới và có thể tận dụng lợi thế kinh tế của điện toán máy tính giá rẻ của lưới. Nhưng với yêu cầu bí mật, thì kỹ thuật này có thể không phải là ứng cử viên tốt do việc phân bổ dữ liệu cho thành viên trong lưới không thể đảm bảo được việc xử lý dữ liệu này không đi ngược lại lợi ích của chủ sở hữu của các thành viên lưới cá nhân. Ngoài ra, vì các thành viên của lưới có năng lực và tính sẵn dùng khác nhau và không tin tưởng lẫn nhau nên tính toán lưới không thích hợp cho các ứng dụng yêu cầu tương tác chặt chẽ và phối hợp giữa nhiều đơn vị khối lượng công việc. Điều này có nghĩa là dữ liệu nhạy cảm không nên được xử lý trên một mạng lưới, và đây không phải là công nghệ thích hợp cho các ứng dụng nhạy cảm với thời gian.

## 5.4 Quản lý sự cố

### 5.4.1 *Khái niệm sự cố*

Nhiều tội phạm máy tính không được báo cáo vì nạn nhân, trong nhiều trường hợp, không biết về vụ việc hoặc chỉ muốn vá lỗ hổng mà tin tặc đã xâm nhập và giữ im lặng thông tin chi tiết để khỏi bij xấu hổ hoặc nguy cơ làm tổn thương danh tiếng của cơ quan/tổ chức. Điều này làm cho việc thống kê thực tế khó khăn hơn về số lượng cuộc tấn công xảy ra mỗi ngày, mức độ thiệt hại gây ra, các loại tấn công và phương pháp đang được sử dụng.

Nhiều loại sự cố (vi rút, tấn công nội gián, tấn công khủng bố, v.v.) tồn tại, và đôi khi đó chỉ là lỗi của con người. Như bản cập nhật được triển khai đã làm hỏng thứ gì đó, ai đó định cấu hình sai thiết bị hoặc quản trị viên vừa học một ngôn ngữ kịch bản mới và tung ra một số mã gây ra tình trạng lộn xộn và nhầm lẫn.

Khi sự cố được phát hiện và người ứng phó với sự cố được chỉ định, việc này thực tế sẽ kích hoạt quy trình ứng phó sự cố. Sự cố được xác định khi ai đó hoặc việc gì đó dẫn đến cảnh báo về vi phạm chính sách của cơ quan/tổ chức hoặc hành động bất hợp pháp.

Véc tơ tấn công là phương tiện mà kẻ tấn công nhắm mục tiêu vào hệ thống máy tính hoặc cá nhân. Tin tặc có thể cố gắng giành quyền truy cập vào hệ thống máy tính bằng cách gửi một email rác tới người dùng, cùng với file đính kèm độc hại. Do đó, kẻ tấn công đang cố gắng thuyết phục người dùng mở gửi email và đọc file đính kèm, do đó

thực thi phần mềm độc hại và lây nhiễm hệ thống đích. Trong trường hợp này, véc tơ tấn công là email spam, với sự kết hợp giữa kỹ thuật xã hội và phần mềm độc hại.

Các véc tơ tấn công là cách thức mà kẻ tấn công sẽ thực hiện để thử và khai thác lỗ hổng bảo mật, Chính vì việc sử dụng các véc tơ này mà nhóm vận hành an toàn của cơ quan/tổ chức sẽ cố gắng phát hiện, đồng thời kích hoạt quy trình ứng phó sự cố. Ngay tại thời điểm kích hoạt, giai đoạn đầu tiên của quá trình ứng phó sự cố được gọi là ngăn chặn. Cơ quan/tổ chức có thể được hưởng lợi đáng kể nhờ việc chuẩn bị đúng cách cho những loại sự cố này. Nhóm vận hành an toàn có khả năng giúp cơ quan/tổ chức duy trì hoạt động trong một cuộc tấn công thực sự. Nhờ việc lập chi tiết công việc cần phải làm gì, cách thức liên lạc và với ai, kế hoạch ứng phó sự cố được kiểm tra một cách kỹ lưỡng là chìa khóa cho sự bền vững của cơ quan/tổ chức, bất kể điều gì dịch vụ cung cấp, thị trường hoạt động, và mục tiêu lớn như thế nào.

Các dữ kiện liên quan đến mỗi sự cố chắc chắn sẽ khác nhau nhưng điều quan trọng là kiểm tra kế hoạch ứng phó với nhiều tình huống để các quy trình ứng phó linh hoạt nhất có thể. Điều này có nghĩa là nhóm ứng phó sự cố sẽ có thể suy nghĩ một cách thấu đáo về các vấn đề cụ thể và xác định, ít nhất là ở các cấp độ của quy trình, phải làm gì trong suốt vòng đời của sự cố. Cuối cùng, liên quan đến việc ứng phó sự cố, đó là tất cả các nhóm và nhân viên hiểu rõ khi xảy ra sự cố nhiệm vụ của mỗi cá nhân ngay cả khi chỉ đơn giản là đăng xuất máy tính. Khi ứng phó với sự cố, các kế hoạch thông tin liên lạc và sẵn sàng cần được hiểu rõ để đảm bảo rằng sự cố được xử lý một cách hiệu quả và nhân viên biết họ nên và không nên thảo luận về sự cố với ai. Trong sự cố nghiêm trọng, việc chuẩn bị cho nhóm quan hệ công chúng những thông điệp soạn sẵn mà họ có thể nói với giới truyền thông là điều cần thiết. Một trong những khía cạnh phi kỹ thuật đầu tiên của việc quản lý bất kỳ sự cố nào là làm việc với nhóm điều hành hoặc giám đốc điều hành để chuẩn bị cho họ trước những câu hỏi khó trên phương tiện truyền thông.

### 5.4.2 *Chuẩn bị*

Việc chuẩn bị quản lý sự cố cần bao gồm việc xác định các cách thức mà kế hoạch ứng phó truyền đạt cho lực lượng lao động trong cơ quan/tổ chức. Kế hoạch truyền thông phải luôn sẵn sàng cho mọi người và điều quan trọng là phải có cả bản sao trực tuyến (được truy cập thông qua mạng nội bộ cơ quan hoặc hệ thống quản lý tài liệu) và bản cứng được đặt ở những vị trí chiến lược trong toàn bộ cơ sở của bạn để trong trường hợp hệ thống bị trục trặc, kế hoạch vẫn có thể truy cập được. Hàng năm cơ quan nên xem xét kế hoạch ứng phó của mình và cập nhật kế hoạch truyền thông, tìm kiếm những vấn đề không phù hợp, những cá nhân đã rời đi và đảm bảo rằng cơ quan xác nhận rằng từng cách thức liên lạc của những người có trách nhiệm cập nhật bao gồm:

- Số điện thoại
- Địa chỉ email
- Trụ sở làm việc
- Số bàn

- Địa chỉ nhà
- Thông tin liên hệ thay thế
- Người dự phòng nếu họ không có mặt

Các chính sách của cơ quan/tổ chức phải chỉ ra cách thức xử lý và báo cáo sự cố, ít nhất là ở mức cao, trong khi các hướng dẫn và tiêu chuẩn phải liệt kê bất kỳ tài liệu tham khảo cần thiết nào mà người quản lý và các thành viên trong nhóm ứng phó sự cố cần. Một khía cạnh của việc công bố chính sách là việc ủy quyền một cách rõ ràng cho nhóm ứng phó sự cố. Điều này có nghĩa là trong thời gian xảy ra sự cố, nhóm ứng phó có các đặc quyền đặc biệt để ngăn chặn, xóa, điều tra và khôi phục dịch vụ, có thể liên quan đến những việc mà trong điều kiện bình thường, họ có thể không được phép làm. Cơ quan/tổ chức nên xem xét hàng năm các chính sách bảo mật của mình để đảm bảo rằng chúng tuân thủ các thay đổi trong luật, trong việc quản trị tổ chức.

### 5.4.3 *Phát hiện và phân tích*

Quan sát và phản ứng với các hoạt động đáng ngờ trong cơ quan/tổ chức là một khía cạnh phức tạp và thường bị bỏ qua của quản lý sự cố. Nếu không có phương tiện phát hiện sự cố, kẻ tấn công có thể xâm nhập hệ thống và duy trì quyền truy cập trong thời gian dài. Nếu không có đủ phương tiện để quan sát trạng thái hệ thống và phân tích trạng thái bảo mật của chúng, cơ quan/tổ chức chỉ có thể biết về sự cố khi nhận được kích hoạt bên ngoài, chẳng hạn như thông tin bí mật xuất hiện trên trang web tấn công hoặc các chi tiết nhạy cảm về cơ quan/tổ chức xuất hiện trên các phương tiện truyền thông.

Các sự kiện log được tạo ra bởi công nghệ hiện đại nhất để chúng có thể được nhập vào bởi các hệ thống giám sát đặc biệt được gọi là hệ thống quản lý sự kiện và thông tin bảo mật (SIEM), cho phép các nhóm vận hành an ninh giám sát môi trường từ một vị trí (trung tâm vận hành an ninh). Các sự kiện bảo mật yêu cầu mức độ phân tích, tự động hoặc bởi người phân tích được đào tạo để hiểu và sử dụng thông tin để phát hiện các mối đe dọa tiềm ẩn. Nếu một sự kiện hoặc cảnh báo được phát hiện được coi là dấu hiệu của sự xâm phạm thì quy trình quản lý sự cố có thể được ban hành. Trung tâm vận hành an ninh trở thành hệ thống cảnh báo sớm sàng lọc hàng trăm nghìn sự kiện log để tìm kiếm các dấu hiệu của sự xâm phạm, dựa trên chữ ký, kinh nghiệm và các quy tắc tương quan được lập trình trước để phát hiện các véc-tơ tấn công đang được sử dụng.

Có hai phương pháp mà nhóm an ninh có thể sử dụng khi điều tra một sự cố tùy thuộc vào hoàn cảnh của sự kiện. Loại đầu tiên được gọi là phân tích tinh (*static analysis*), thường cần sử dụng các công cụ phần mềm đặc biệt để xem phần mềm độc hại nào được cài đặt trên hệ thống và cách phần mềm độc hại đó có thể hoạt động. Tuy nhiên, phần mềm độc hại sẽ không được thực thi để xem xét hành vi của nó. Hình thức điều tra thứ hai liên quan đến việc thiết lập một môi trường thử nghiệm đặc biệt và sau đó chạy phần mềm độc hại, để có thể ghi lại phần mềm độc hại làm gì và sử dụng những kết quả đó để xác định cách nó hoạt động và tác động của nó đối với mục tiêu. Việc phân tích động đôi khi còn được gọi là phân tích hành vi.

### 5.4.4 *Ngăn chặn và khôi phục*

Sau khi giai đoạn phân tích kết thúc, nhóm ứng phó sự cố sẽ xem xét các cách để ngăn chặn tác động của sự cố và giải quyết nó một cách sạch sẽ và hiệu quả nhất có thể. Kế hoạch ngăn chặn được cân nhắc tốt sẽ giúp giảm thiểu tác động của sự cố đối với hoạt động của cơ quan/tổ chức, nhưng trong thời gian gấp rút, chẳng hạn như đợt bùng phát vi rút, cần đảm bảo rằng không để mất các nguồn bằng chứng quan trọng, chẳng hạn như bộ nhớ có thể xóa.

Một chiến lược ngăn chặn phù hợp giúp nhóm ứng phó sự cố có thời gian để điều tra thích hợp và xác định nguyên nhân gốc rễ của sự cố. Chiến lược ngăn chặn phải dựa trên loại tấn công (nghĩa là cuộc tấn công bên trong hay bên ngoài), tài sản bị ảnh hưởng bởi sự cố và mức độ nghiêm trọng của những tài sản đó. Các chiến lược ngăn chặn có thể mang tính chủ động hoặc đối phó phụ thuộc vào môi trường và loại cuộc tấn công. Trong một số trường hợp, hành động tốt nhất có thể là ngắt kết nối hệ thống bị ảnh hưởng khỏi mạng. Tuy nhiên, cách tiếp cận đối phó này có thể gây ra từ chối dịch vụ hoặc hạn chế chức năng của các hệ thống quan trọng.

Khi cách ly hoặc ngăn chặn hoàn toàn không khả thi, có thể chọn sử dụng phân đoạn mạng để cô lập một hệ thống hoặc nhiều hệ thống. Các thiết bị tại ranh giới cũng có thể được sử dụng để ngăn hệ thống này lây nhiễm sang hệ thống khác. Một chiến lược đối phó khác liên quan đến việc xem xét và sửa đổi cấu hình bộ định tuyến/bộ lọc tường lửa. Danh sách kiểm soát truy cập cũng có thể được áp dụng để giảm thiểu khả năng phơi nhiễm. Các chiến lược ngăn chặn này cho kẻ tấn công biết rằng cuộc tấn công của hắn đã được chú ý và các biện pháp đối phó đang được thực hiện. Để thực hiện phân tích nguyên nhân gốc rễ, người ta cần giữ cho hệ thống bị ảnh hưởng trực tuyến và không để lộ cuộc tấn công đã bị chú ý, người ta có thể cân nhắc việc cài đặt bẫy *honeypot* để dành ra một khu vực có thể chịu tấn công nhưng gây ra rủi ro tối thiểu cho tổ chức.

Một trong những thách thức lớn nhất mà nhóm vận hành an toàn phải đối mặt là tính chất động của các bản ghi log. Nhiều hệ thống được định cấu hình để xóa hoặc ghi đè log trong một khung thời gian ngắn và thời gian sẽ bị mất ngay khi sự cố xảy ra. Vài giờ đã có thể trôi qua trước khi sự cố được báo cáo hoặc phát hiện. Một số quốc gia đang xem xét luật yêu cầu lưu giữ file log lâu hơn. Tuy nhiên, những luật như vậy đặt ra những thách thức về quyền riêng tư và lưu trữ.

Khi có nhiều thông tin và trả lời nhiều câu hỏi nhất có thể, giai đoạn theo dõi bắt đầu. Việc theo dõi cũng có thể diễn ra song song với việc phân tích và kiểm tra. Cần xác định xem nguồn gốc của vụ việc là bên trong hay bên ngoài và cách thức kẻ phạm tội thâm nhập và tiếp cận tài sản. Nếu kẻ tấn công là bên ngoài, nhóm sẽ liên hệ với nhà cung cấp dịch vụ ISP để thu thập dữ liệu và tìm ra nguồn gốc của cuộc tấn công. Nhiều khi điều này rất khó vì những kẻ tấn công di chuyển từ hệ thống này sang hệ thống khác, vì vậy một số ISP có thể phải tham gia. Do đó, điều quan trọng là nhôm vận hành an toàn phải

có mối quan hệ làm việc tốt với các bên thứ ba như ISP, các nhóm phản ứng khác và cơ quan thực thi pháp luật

Việc phục hồi hoạt động của cơ quan/tổ chức là quá trình đưa doanh nghiệp trở lại hoạt động bình thường. Phần lớn quá trình khôi phục liên quan đến việc người quản trị đưa hệ thống về trạng thái trước khi xảy ra sự cố, chẳng hạn như khôi phục hệ thống từ bản sao lưu, chạy tập lệnh hoặc quy trình thiết lập lại quyền truy cập hệ thống và truy cập mạng và đảm bảo rằng cơ quan/tổ chức có thể quay trở lại trạng thái trước khi xảy ra cuộc tấn công hoặc nhận ra nguy cơ. Trong trường hợp nhiều hệ thống máy tính bị ảnh hưởng bởi phần mềm độc hại, chẳng hạn như trong đợt bùng phát phần mềm độc hại hoặc ransomware, một số quản trị sẽ thực hiện cài đặt mới môi trường điều hành tiêu chuẩn (hệ điều hành và các ứng dụng tiêu chuẩn) vì thực hiện việc này nhanh hơn là cố gắng xử lý một hệ thống bị lây nhiễm. Vấn đề là rất khó để đảm bảo phần mềm độc hại đã bị xóa hoàn toàn (một số phần mềm lây nhiễm đủ thông minh để ẩn nhiều bản sao của chính chúng và có thể nằm im trong tuần hoặc thậm chí hàng tháng mà không bị phát hiện).

Sau khi khắc phục sự cố, cần lập hồ sơ, báo cáo và đánh giá hiệu quả của kế hoạch ứng phó. Các loại báo cáo có thể sẽ cần tạo bao gồm nhật ký phân tích về cách xử lý sự cố, thông qua báo cáo kết thúc phân tích và định lượng hiệu quả của từng giai đoạn của kế hoạch. Cơ quan/tổ chức sẽ cần phải xem xét tất cả các khía cạnh của phương pháp, kỹ thuật, phương pháp luận và phát hiện liên quan đến sự cố này. Do có nhiều bên liên quan đối với các báo cáo này nên chúng cần phải rõ ràng, ngắn gọn và không có những thuật ngữ kỹ thuật không cần thiết.

### 5.4.5 *Triển khai các biện pháp phát hiện và ngăn chặn*

Một cách lý tưởng, cơ quan/tổ chức có thể tránh hoàn toàn các sự cố bằng cách thực hiện các biện pháp đối phó mang tính phòng ngừa. Khi sự cố xảy ra, cơ quan/tổ chức muốn phát hiện ra càng sớm càng tốt. Hệ thống phát hiện và ngăn chặn xâm nhập là một trong những biện pháp mà cơ quan/tổ chức có thể thực hiện để phát hiện và ngăn chặn thành công các cuộc tấn công. Mặc dù không có biện pháp đơn giản nào có thể thực hiện để bảo vệ khỏi tất cả các cuộc tấn công, nhưng có một số bước cơ bản cơ quan/tổ chức có thể thực hiện để bảo vệ khỏi nhiều loại tấn công như được liệt kê ở dưới đây.

*Luôn cập nhật hệ thống và ứng dụng*. Các nhà cung cấp thường xuyên phát hành các bản vá để sửa lỗi và lỗi bảo mật, nhưng những bản vá này chỉ hữu ích khi chúng được áp dụng. Quản lý bản vá đảm bảo rằng các hệ thống và ứng dụng luôn được cập nhật với các bản vá có liên quan.

*Xóa hoặc tắt các dịch vụ và giao thức không cần thiết*. Nếu một hệ thống không cần dịch vụ hoặc giao thức, hệ thống đó sẽ không chạy. Những kẻ tấn công không thể khai thác lỗ hổng trong một dịch vụ hoặc giao thức không chạy trên hệ thống. Ngược lại, máy chủ web đang chạy mọi dịch vụ và giao thức có sẵn, nó dễ bị tấn công tiềm ẩn vào bất kỳ dịch vụ và giao thức nào trong số này.

*Sử dụng hệ thống phát hiện và ngăn chặn xâm nhập*. Hệ thống phát hiện và ngăn chặn xâm nhập quan sát hoạt động, cố gắng phát hiện các cuộc tấn công và đưa ra cảnh báo. Chúng thường có thể chặn hoặc ngăn chặn các cuộc tấn công.

*Sử dụng phần mềm chống phần mềm độc hại cập nhật*. Một biện pháp đối phó chính là phần mềm chống phần mềm độc hại cho phép phát hiện và loại bỏ các phần mềm độc hại khỏi máy tính và hệ thống. Điểm mấu chốt là sử dụng các phiên bản cập nhật kịp thời để ứng phó được với các dạng mã độc mới.

*Sử dụng tường lửa*. Tường lửa có thể ngăn chặn nhiều kiểu tấn công khác nhau. Tường lửa cho mạng bảo vệ toàn bộ mạng và tường lửa cho máy chủ bảo vệ các hệ thống riêng lẻ.

*Thực hiện các quy trình cấu hình và quản lý hệ thống*. Các quy trình quản lý hệ thống và kiểm duyệt cấu hình giúp đảm bảo rằng các hệ thống được triển khai một cách an toàn và duy trì ở trạng thái an toàn trong suốt vòng đời của chúng.

## 5.5 Trách nhiệm trong quản lý vận hành, khai thác

Nỗ lực liên tục mà cơ quan/tổ chức luôn cố gắng thực hiện nhằm đảm bảo các chính sách, thủ tục, tiêu chuẩn và hướng dẫn chính xác được đưa ra và tuân thủ là một phần quan trọng trong các hoạt động an toàn của mình. Việc chuyên cần và cẩn trọng phải được thực hiện theo cách có trách nhiệm, cẩn thận, thận trọng và thực tế. Các bước đúng đắn cần được thực hiện để đạt được mức độ bảo mật cần thiết, đồng thời cân bằng tính dễ sử dụng với việc tuân thủ các yêu cầu pháp lý cũng như ràng buộc chi phí để duy trì mức độ an toàn thích hợp. Việc vận hành an toàn đảm bảo rằng con người, ứng dụng, thiết bị và môi trường tổng thể được an toàn đúng mức và đầy đủ.

Mặc dù vận hành an toàn duy trì việc luyện tập thường xuyên để giữ cho môi trường hoạt động ở mức độ bảo mật cần thiết, các liên đới và trách nhiệm pháp lý cũng tồn tại khi thực hiện các nhiệm vụ này. Các cơ quan và giám đốc điều hành cấp cao tại các cơ quan này thường có nghĩa vụ pháp lý để đảm bảo rằng các nguồn lực được bảo vệ, các biện pháp an toàn được thực hiện và các cơ chế bảo mật được kiểm tra để đảm bảo họ đang thực sự cung cấp mức độ bảo vệ cần thiết.

Việc quản lý hành chính là một phần rất quan trọng của vận hành an toàn. Một khía cạnh của quản lý hành chính cần xử lý các vấn đề nhân sự. Điều này bao gồm việc tách nhiệm vụ và luân phiên công việc. Mục tiêu của việc phân chia nhiệm vụ là đảm bảo rằng người vận hành một mình không thể xâm phạm an ninh của cơ quan theo bất kỳ cách nào. Các hoạt động có nguy cơ cao nên được chia thành các phần khác nhau và được phân phối cho các cá nhân hoặc phòng ban khác nhau. Bằng cách đó, cơ quan/tổ chức không phải đặt độ tin cậy một cách đầy rủi ro lên một số cá nhân nhất định.

Phần dưới đây trình bày về vai trò và chức trách căn bản của các bộ phận tiêu biểu cũng như của bộ phận CNTT trong việc vận hành an toàn của cơ quan/tổ chức:

- Quản lý điều hành

- Giám sát và điều chỉnh chiến lược an toàn
- Có trách nhiệm về tổ chức thực hiện toàn bộ các phần của chương trình an toàn được yêu cầu

- Quản lý rủi ro kinh doanh
  - Đánh giá rủi ro về CNTT
  - Lập danh sách ưu tiên các rủi ro CNTT để được xử lý. Danh sách này được duy trì và cập nhật định kỳ
- Quản lý phòng ban
  - Ký nhận các yêu cầu an toàn và kiểm tra tính chấp nhận được. Như ác tính năng an toàn cần được tích hợp vào trong ứng dụng phải được phê duyệt chính thức
  - Xác thực việc truy nhập: Cá nhân hay nhóm cần truy nhập tới dữ liệu cần được phê duyệt chính thức
- Tư vấn pháp lý cho quản lý điều hành:
  - Tư vấn bảo vệ thông tin. Các chính sách bảo vệ thông tin cần nhất quán với luật pháp, quy định, được phê duyệt chính thức và người chịu ảnh hưởng phải có nhận thức về các chính sách này
- Quản lý vận hành CNTT
  - Giám sát an toàn: xác định các sự vụ an toàn trước khi chúng có thể xảy ra
  - Ứng phó sự vụ: Phản ứng thích đáng với các sự vụ an toàn được nêu trong các thủ tục vận hành
  - Quản lý khủng hoảng: Thủ tục phục hồi được kiểm tra thành công và định kỳ
  - Kiểm kê vị trí (site): Các thiết bị tính toán được mua, được xác định và liên quan tới mục đích kinh doanh
- Quản lý chất lượng
  - Tham gia đánh giá an toàn: cấu hình hệ thống tuân thủ chính sách an toàn
  - Xây dựng các yêu cầu an toàn: Các yêu cầu kinh doanh về tính bí mật, toàn vẹn, sẵn dùng cần được lập tài liệu
  - Thiết kế an toàn ứng dụng: thu xếp các kế hoạch triển khai về mặt kỹ thuật để đáp ứng các yêu cầu an toàn quy trình kinh doanh
  - Kiểm soát thay đổi: lưu trữ, tìm kiếm an toàn và lập kế hoạch cho việc duy trì mã nguồn cũng như tùy biến sản phẩm
  - Quản lý nâng cấp an toàn: Đảm bảo việc kiểm tra và áp dụng vá lỗ hổng phần mềm
- Mua sắm (vật tư)

- Mô tả các yêu cầu an toàn: Các yêu cầu chính thức về an toàn đối với toàn bộ sản phẩm cũng như các đề xuất
- Yêu cầu liên lạc: yêu cầu về bí mật, toàn vẹn và sẵn dùng với các nhà cung cấp dịch vụ và hợp đồng bảo trì kỹ thuật.

## 5.6 Câu hỏi ôn tập

1. Trình bày các nguyên tắc căn bản với việc vận hành an toàn.
2. Hãy nêu các công việc/nhiệm vụ cơ bản với vận hành an toàn.
3. Trình bày các bước cơ bản của quy trình kiểm soát thay đổi.
4. Hãy nêu các tình huống cơ bản làm cấu hình hệ thống thay đổi. Cho ví dụ.
5. Với các vị trí công việc khác nhau như: quản trị mạng, quản trị cơ sở dữ liệu sẽ phải xử lý các thay đổi như thế nào.
6. Trình bày các vấn đề với việc hủy bỏ dữ liệu an toàn.
7. Nêu một số ví dụ về việc huỷ bỏ dữ liệu an toàn.
8. Trinhg bày các biện pháp đảm bảo tính sẵn dùng của mạng và các tài nguyên.
9. Việc sử dụng kỹ thuật nhóm khác biệt gì với kỹ thuật mạng lưới cũng như điện toán đám mây.
10. Trình bày khái niệm sự cố.
11. Trình bày các bước ứng phó với sự cố.
12. Nêu các biện pháp cơ bản hạn chế lỗ hổng an toàn khi xử lý sự cố.

# CHƯƠNG 6. DUY TRÌ HOẠT ĐỘNG VÀ KHẮC PHỤC SỰ CỐ

Sự cố hay thảm họa do thiên tai hay con người tác động tới mọi cơ quan/tổ chức và đe dọa việc hoạt động bình thường thậm chí phá hủy toàn bộ các hoạt động của cơ quan/tổ chức. Để tồn tại và vượt qua sự cố, cơ quan/tổ chức cần có tầm nhìn xa, lập kế hoạch, ước lượng tổn hại và thiết lập biện pháp bảo vệ. Chương này tập trung vào vấn đề xử lý và đối phó với những tình huống sự cố. Đồng thời giới thiệu cách thức xây dựng các kế hoạch để khôi phục hệ thống khi sự cố cũng như đảm bảo khả năng hoạt động của hệ thống trong tình huống tài nguyên hạn chế.

## 6.1 Nguyên tắc duy trì hoạt động và khắc phục sự cố

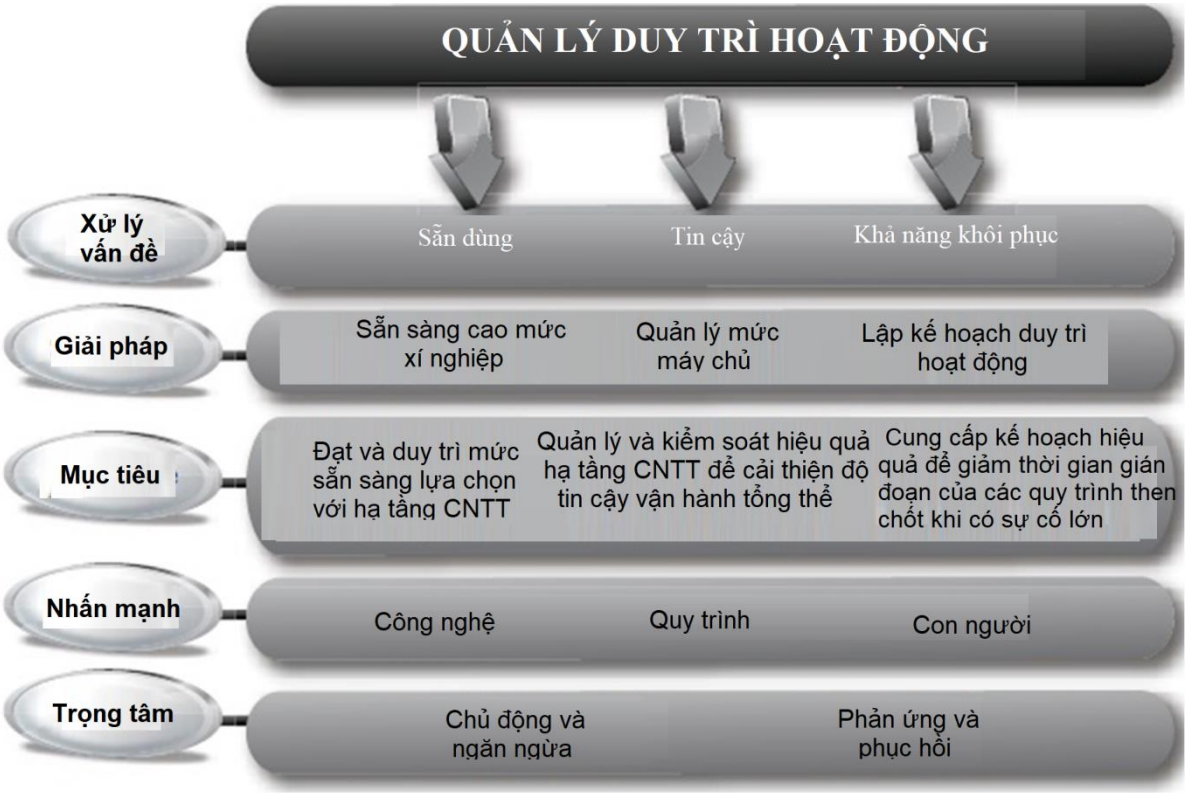
Từ góc độ quản trị để đối phó với sự cố, các cơ quan/tổ chức cần phải làm tất cả mọi biện pháp có thể một cách chủ động để tránh bất kỳ thảm họa, thậm chí mọi thảm họa dự kiến. Đối với việc lập kế hoạch, cần giả định rằng thảm họa dự kiến là không thể tránh khỏi. Lập kế hoạch hành động phản ứng để cho cơ quan/tổ chức sẽ tồn tại và tiếp tục hoạt động sản xuất cho các thế hệ tiếp theo dù thảm họa không thể tránh khỏi và kết quả là tổn thất tai hại.

Mục tiêu của việc *khôi phục sau sự cố* (thảm họa) là giảm thiểu hậu quả của sự cố hay gián đoạn, nghĩa là cần tiến hành các bsước có thể để đảm bảo các tài nguyên, nhân sự, và quy trình hoạt động có khả năng khôi phục theo cách kịp thời. Điều này khác với *lập kế hoạch duy trì* mà việc này cung cấp các biện pháp và thủ tục để xử lý các sự cố và việc gián đoạn lâu dài. Kế hoạch khôi phục thảm họa nhằm xử lý thảm họa và các hệ quả của nó ngay sau khi thảm họa xảy ra; kế hoạch khôi phục thảm họa thường tập trung vào công nghệ thông tin.

*Kế hoạch khôi phục thảm họa* được thực hiện khi tất cả mọi thứ vẫn còn trong chế độ khẩn cấp, và tất cả mọi người đang nỗ lực để toàn bộ các hệ thống quan trọng hoạt động trở lại. *Kế hoạch duy trì hoạt động* có cách tiếp cận rộng hơn cho vấn đề trên. Kế hoạch này có thể bao gồm việc đưa các hệ thống quan trọng vào môi trường khác trong khi việc sửa chữa các phương tiện ban đầu đang được tiến hành, và đưa đúng người đến đúng nơi đúng lúc và thực hiện các hoạt động của cơ quan/tổ chức ở chế độ khác cho đến khi các điều kiện bình thường được khôi phục lại. Kế hoạch cũng liên quan đến việc liên lạc với khách hàng, đối tác và cổ đông thông qua các kênh khác nhau cho đến khi mọi thứ trở lại bình thường. Vì vậy, khắc phục thảm họa đối phó với các diễn tiến của thảm họa hay sự cố trong khi việc lập kế hoạch duy trì đối phó các hậu quả của các sự kiện không mong muốn này.

Trong khi k*ế hoạch khôi phục thảm họa* và k*ế hoạch duy trì hoạt động* hướng đến xây dựng các kế hoạch, *quản lý duy trì hoạt động* là quy trình quản lý toàn diện cần bao

gồm cả hai công việc trên. Quản lý duy trì hoạt động cung cấp khung khuôn khổ để tích hợp khả năng phục hồi với khả năng đáp ứng hiệu quả nhằm bảo vệ lợi ích của các bên liên quan chính của cơ quan/tổ chức. Mục tiêu chính của *quản lý duy trì hoạt động* là cho phép cơ quan/tổ chức tiếp tục thực hiện các hoạt động của mình trong các điều kiện khác nhau.




**Hình 6-1. Các bước quản lý hoạt động liên tục.**

Với việc đảm bảo hoạt động liên tục, tính toàn vẹn và bảo mật phải được xem xét không chỉ trong các thủ tục hàng ngày, mà còn cần được xem xét trong thảm họa hoặc gián đoạn. Ví dụ có thể không phù hợp khi bỏ máy chủ lưu giữ thông tin quan trọng khi mọi người khác chuyển sang vị trí khác. Tương tự, thiết bị cung cấp kết nối mạng riêng ảo an toàn có thể bị phá hủy và nhóm khôi phục tập trung vào chức năng truy cập từ xa nhưng quên yêu cầu mã hóa. Nếu bảo mật không được tích hợp và triển khai đúng cách, các tác động của thảm họa vật lý có thể bị khuếch đại khi tin tặc xâm nhập và ăn cắp thông tin nhạy cảm. Cơ quan/tổ chức dễ bị tổn thương hơn sau khi thảm họa xảy ra bởi vì các dịch vụ bảo vệ được sử dụng để bảo vệ nó có thể không có sẵn hoặc hoạt động với công suất giảm. Do đó, điều quan trọng là nếu doanh nghiệp có nội dung bí mật thì điều đó sẽ giữ bí mật.

Tính sẵn dùng là một trong những chủ đề chính đằng sau việc lập kế hoạch duy trì hoạt động ở chỗ nó đảm bảo rằng các nguồn lực cần thiết để giữ cho cơ quan/tổ chức tiếp tục sẵn sàng cho người hay hệ thống dựa vào chúng. Điều này có nghĩa là các bản sao lưu cần phải được thực hiện một cách nhất quán, và việc dự phòng đó cần phải được đưa

vào kiến trúc của các hệ thống, mạng và các hoạt động. Nếu các đường liên lạc bị vô hiệu hóa hoặc nếu một dịch vụ không sử dụng được trong bất kỳ khoảng thời gian đáng kể nào thì phải có biện pháp nhanh chóng và thử nghiệm để thiết lập các dịch vụ và thông tin liên lạc thay thế.

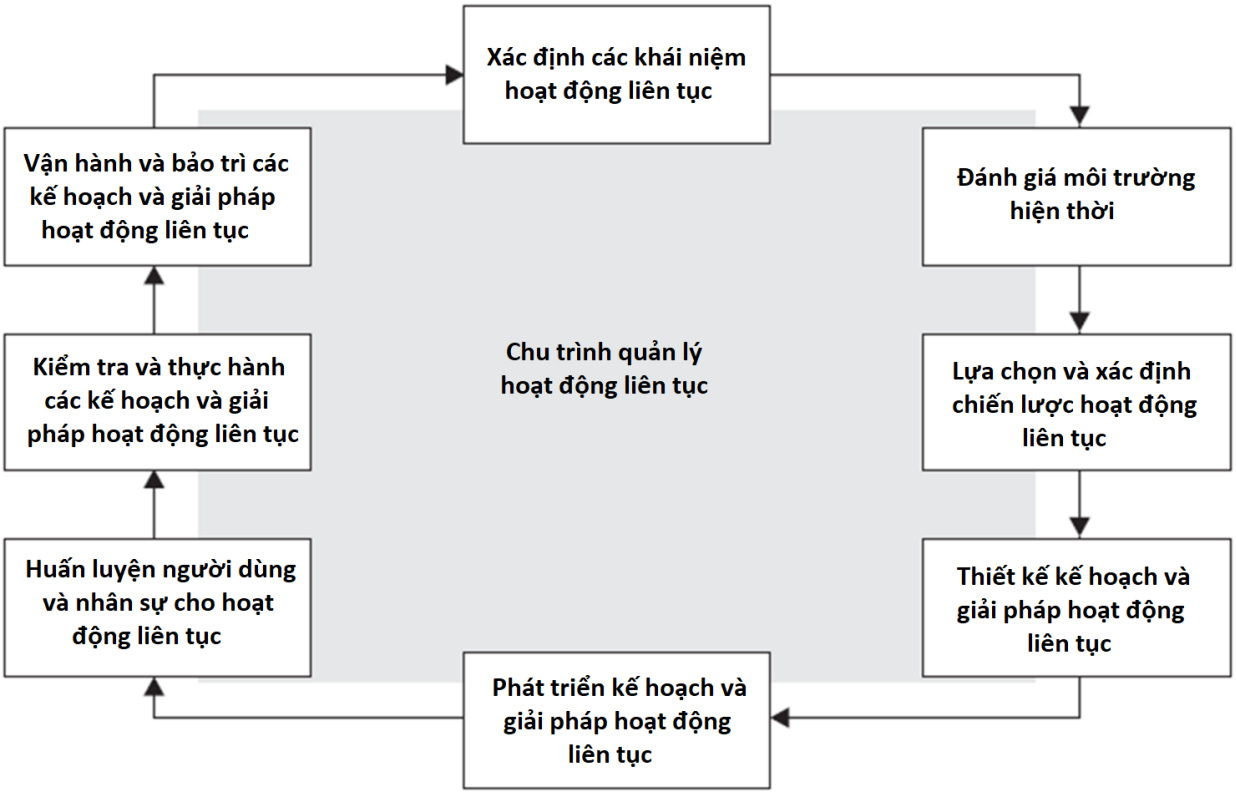
Khi xem xét kế hoạch hoạt động hay kinh doanh, một số cơ quan/tổ chức tập trung chủ yếu vào việc sao lưu dữ liệu và đảm bảo phần cứng dự phòng. Mặc dù những mục này cực kỳ quan trọng nhưng chúng chỉ là những phần nhỏ trong hoạt động tổng thể của cơ quan/tổ chức. Phần cứng và máy tính cần con người cấu hình và vận hành chúng, và dữ liệu sẽ không hữu ích trừ khi chúng có thể truy cập được bởi các hệ thống khác và có thể là các đối tượng bên ngoài. Việc lập kế hoạch phải bao gồm đưa đúng người đến đúng địa điểm, ghi lại các cấu hình cần thiết, thiết lập các kênh truyền thông thay thế (thoại và dữ liệu), đảm bảo năng lượng và cần chắc chắn tất cả các phụ thuộc được hiểu và xem xét một cách thích đáng.

Điều quan trọng để hiểu làm thế nào các công việc tự động được thực hiện một cách thủ công, khi cần thiết, và làm thế nào các quy trình hoạt động có thể được thay đổi một cách an toàn để giữ cho hoạt động của cơ quan/tổ chức tiếp tục. Vấn đề này có thể rất quan trọng trong việc đảm bảo sự tồn tại của cơ quan/tổ chức với sự kiện đó và ít tác động nhất đến hoạt động cơ quan/tổ chức. Nếu không có tầm nhìn và lập kế hoạch, khi một thảm họa xảy ra, dù có thể có dữ liệu dự phòng và các máy chủ dự phòng sẵn sàng tại vị trí thay thế, nhưng những người chịu trách nhiệm kích hoạt chúng có thể đứng quanh trong trạng thái mất bình tĩnh hay không biết bắt đầu từ đâu hoặc cách thực hiện trong môi trường khác biệt như vậy.

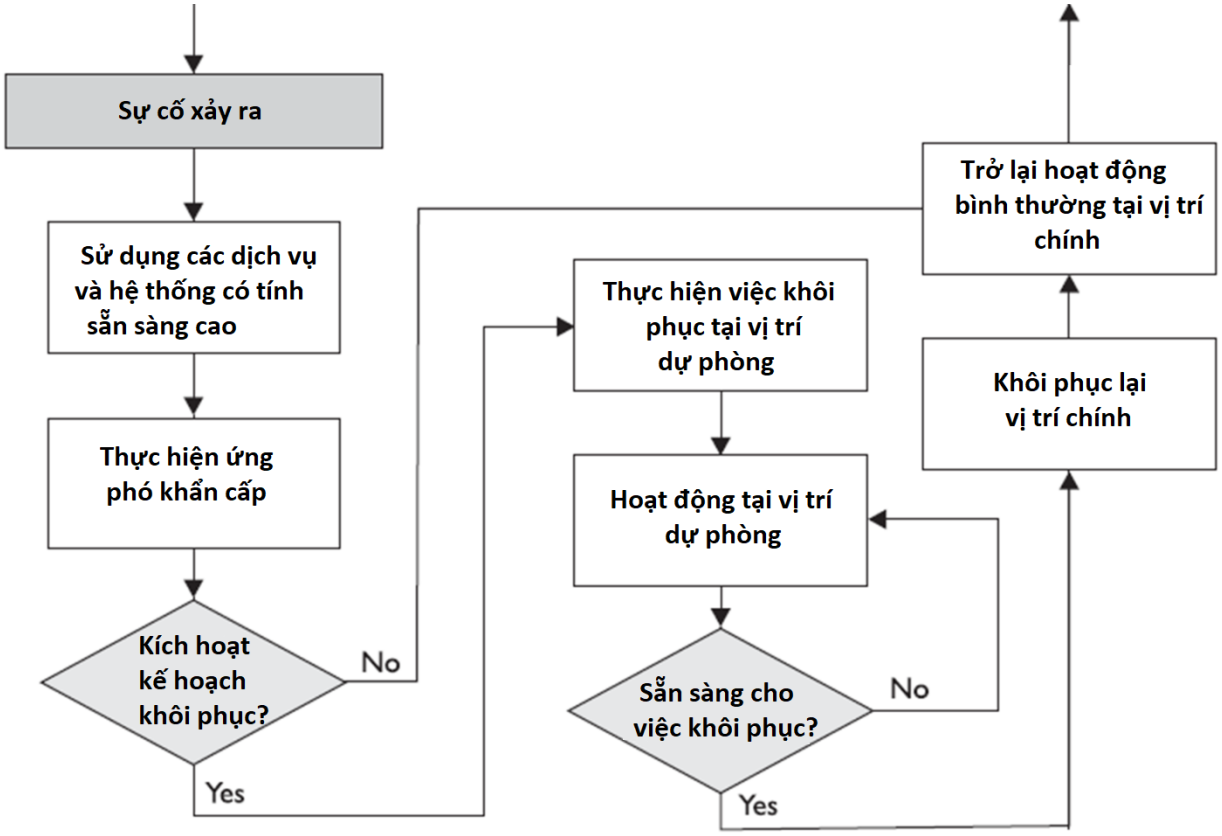
Các biện pháp và thủ tục sắp đặt trước ứng phó với sự cố cho phép:

- Đảm bảo biện pháp phản ứng tức thì và thích hợp với các tình huống nguy cấp
- Bảo vệ tính mạng cho mọi người và đảm bảo an toàn
- Giảm thiểu tác động đến công việc
- Khôi phục hoạt động các chức năng hoạt động/kinh doanh thiết yếu
- Làm việc với các nhà cung cấp và đối tác trong quá trình khôi phục
- Giảm nhiễu loạn trong khi khủng hoảng
- Đảm bảo khả năng sống sót của công việc/kinh doanh
- Khôi phục và hoạt động trở lại nhanh chóng sau thảm họa

Khi xây dựng các kế hoạch thì không có phương thức mang tính khoa học mà chỉ có kinh nghiệm thực tế đã được chứng tỏ theo thời gian. Tuy nhiên, các tổ chức tiêu chuẩn như NIST hay ISO đã đưa ra các khuyến cáo mà một số tổ chức hay cơ quan bắt buộc tuân thủ. Hình 6-2 và Hình 6-3 dưới đây thể hiện các bước tiêu biểu trong quy trình quản lý nhằm đảm bảo hoạt động liên tục và ứng phó khi có sự cố xảy ra.




**Hình 6-2. Chu trình quản lý hoạt động liên tục.**




**Hình 6-3. Quy trình khôi phục sự cố**

## 6.2 Xây dựng kế hoạch duy trì hoạt động

Mục tiêu cuối cùng của việc xây dựng kế hoạch duy trì hoạt động là đưa ra phản ứng bình tĩnh, nhanh chóng, hiệu quả khi có sự việc khẩn cấp và tăng cường khả năng khôi phục một cách mau lẹ của cơ quan/tổ chức khi có sự cố gián đoạn.

Việc xây dựng kế hoạch duy trì hoạt động bao gồm 4 bước chính:

- Lập kế hoạch và phạm vi dự án
- Đánh giá tác động tới công việc
- Lập kế hoạch duy trì hoạt động
- Phê chuẩn và triển khai

Chi tiết các bước được trình bày trong các phần sau đây.

### 6.2.1 *Lập kế hoạch và phạm vi dự án*

Như với bất kỳ quy trình hoạt động chính tắc nào, việc phát triển một kế hoạch duy trì hoạt động chắc chắn đòi hỏi phải sử dụng phương pháp đã được chứng minh. Điều này đòi hỏi những điều sau đây:

- Phân tích có tổ chức các hoạt động của cơ quan/tổ chức trên quan điểm lập kế hoạch khủng hoảng
- Xây dựng nhóm làm việc được ban lãnh đạo phê chuẩn
- Đánh giá các tài nguyên hiện có cho các hoạt động liên tục
- Phân tích các yếu tố quy định và luật pháp mà chi phối các phản ứng của cơ quan/tổ chức khi có sự vụ khẩn cấp.

a. *Phân tích tổ chức hoạt động*

Một trong những trách nhiệm đầu tiên của các cá nhân chịu trách nhiệm lập kế hoạch duy trì hoạt động là thực hiện phân tích của tổ chức hoạt động để xác định tất cả các phòng ban và cá nhân có liên quan trong quá trình xây dựng kế hoạch. Dưới đây là một số lĩnh vực cần xem xét:

- Các phòng ban hoạt động chịu trách nhiệm về các dịch vụ cốt lõi mà cơ quan/tổ chức cung cấp cho các khách hàng của mình
- Các dịch vụ hỗ trợ quan trọng, chẳng hạn như bộ phận công nghệ thông tin (CNTT), bộ phận bảo trì và các nhóm khác chịu trách nhiệm bảo trì các hệ thống hỗ trợ các phòng ban hoạt động
- Giám đốc điều hành cấp cao và các cá nhân quan trọng khác cần thiết cho khả năng tồn tại liên tục của cơ quan/tổ chức

Quá trình phân tích này rất quan trọng vì hai lý do. Đầu tiên, nó cung cấp nền tảng cần thiết để giúp xác định các thành viên tiềm năng của nhóm xây dựng kế hoạch. Thứ hai, nó cung cấp nền tảng cho phần còn lại của quy trình lập kế hoạch.

Thông thường, phân tích tổ chức hoạt động được thực hiện bởi các cá nhân lãnh đạo nhằm xây dựng kế hoạch duy trì hoạt động. Tuy nhiên, việc xem xét kỹ lưỡng phân tích này phải là một trong những nhiệm vụ đầu tiên được giao cho nhóm xây dựng kế hoạch duy trì hoạt hoạt động một cách đầy đủ. Bước này rất quan trọng vì các cá nhân thực hiện phân tích ban đầu có thể đã bỏ qua các chức năng hoạt động quan trọng mà cần được các thành viên nhóm BCP biết đến. Nếu nhóm tiếp tục mà không sửa đổi phân tích tổ chức thì toàn bộ quá trình lập kế hoạch có thể bị ảnh hưởng tiêu cực và dẫn đến việc xây dựng một kế hoạch không giải quyết đầy đủ các nhu cầu ứng phó khẩn cấp của tổ chức nói chung.

b. *Xây dựng nhóm làm việc*

Trong nhiều tổ chức, các phòng CNTT hay an ninh được giao trách nhiệm duy nhất cho việc lập kế hoạch duy trì hoạt động và không có sự sắp xếp nào cho việc thu thập các thông tin đầu vào từ các bộ phận hoạt động và hỗ trợ khác. Trên thực tế, các phòng ban đó thậm chí có thể không biết về sự tồn tại của kế hoạch cho đến khi sự cố hay thảm họa xảy ra hoặc sắp xảy ra. Đây là một lỗ hổng quan trọng: kiến thức hay chuyên gia về lĩnh vực CNTT là không đủ. Sự phát triển kế hoạch duy trì hoạt động một cách cô độc có thể gây thảm họa theo hai cách. Thứ nhất, bản thân kế hoạch có thể không tính đến tri thức của các cá nhân chịu trách nhiệm cho hoạt động hàng ngày của tổ chức. Thứ hai, nó giữ các yếu tố về các chi tiết cụ thể của kế hoạch  hoạt động liên tục "trong bóng tối" cho đến khi việc thực hiện trở nên cần thiết. Điều này làm giảm khả năng các yếu tố hoạt động sẽ tuân thủ các quy định của kế hoạch và thực hiện một cách hiệu quả. Việc này cũng không cho phép các tổ chức thu được những lợi ích từ chương trình đào tạo và kiểm tra cho kế hoạch đó.

Để ngăn chặn những tình huống này ảnh hưởng xấu đến quá trình lập kế hoạch, các cá nhân chịu trách nhiệm cần đặc biệt quan tâm khi chọn nhóm lập kế hoạch duy trì hoạt động. Ở mức tối thiểu, nhóm nghiên cứu nên bao gồm các cá nhân sau đây:

- Các phòng ban chịu trách nhiệm về các hoạt động cốt lõi của cơ quan/tổ chức
- Các phòng ban hỗ trợ then chốt được xác định qua việc phân tích hoạt động của tổ chức
- CNTT có chuyên môn về lĩnh vực lập kế hoạch duy trì hoạt động
- Phụ trách luật pháp có hiểu biết về trách nhiệm hợp đồng, quy định, luật pháp về doanh nghiệp
- Đại diện từ ban lãnh đạo

Ở góc độ khác, nhiều cơ quan/tổ chức bị ràng buộc với luật pháp hay các quy định của chính quyền địa phương trong việc thực hiện các kế hoạch duy trì hoạt động như quân đội, công an, viễn thông hay điện lực. Mặt khác, các cơ quan/tổ chức bị ràng buộc với khách hàng của mình trong tình huống khẩn cấp thể hiện trong hợp đồng với khách

hàng dưới dạng các thỏa thuận về chất lượng dịch vụ trong các trường hợp phá vỡ việc đảm bảo chất lượng dịch vụ.

### 6.2.2 *Đánh giá tác động*

Việc đánh giá tác động xác định các tài nguyên quan trọng đối với khả năng tồn tại liên tục của cơ quan/tổ chức và các mối đe dọa đặt ra cho các tài nguyên đó. Việc này cũng đánh giá khả năng mà mỗi mối đe dọa sẽ thực sự xảy ra và tác động đến những sự kiện đó sẽ có trong quá trình hoạt động. Kết quả của đánh giá tác động cung cấp các đánh giá định lượng để có thể ưu tiên các nguồn lực cho việc duy trì hoạt động cho các rủi ro cục bộ, khu vực, và toàn cầu đối với cơ quan/tổ chức.

Các mối đe dọa được mô tả thông qua:

- Thời gian chịu đựng tối đa và gián đoạn với các hoạt động
- Gián đoạn hoạt động và năng suất
- Các đánh giá về tài chính
- Trách nhiệm theo quy định
- Mức độ tín nhiệm (danh tiếng)

a. *Đánh giá mức độ chắc chắn*

Sau xác định danh sách các mối đe dọa tiềm tàng tới việc duy trì các hoạt động, một số mối đe dọa có nhiều khả năng xảy ra hơn những mối đe dọa khác. Ví dụ, cơ quan/tổ chức vùng cao có nhiều khả năng phải đối mặt với nguy cơ bị lũ lụt hơn. Để xem xét những khác biệt này, giai đoạn tiếp theo của đánh giá tác động xác định khả năng xảy ra từng rủi ro. Để duy trì tính toán nhất quán, đánh giá này thường được thể hiện dưới dạng tỷ lệ xuất hiện hàng năm phản ánh số lần cơ quan/tổ chức dự kiến gặp phải sự cố nhất định mỗi năm.

Nhóm xây dựng kế hoạch cần ngồi lại và xác định mức độ chắc chắn cho từng rủi ro được xác định trong phần trước. Những con số này phải dựa trên lịch sử cơ quan/tổ chức, kinh nghiệm chuyên môn của các thành viên trong nhóm và lời khuyên từ các chuyên gia, chẳng hạn như các nhà khí tượng học, địa chấn học, chuyên gia phòng cháy và các chuyên gia tư vấn khác khi cần thiết.

b. *Đánh giá tác động*

Việc đánh giá rủi ro được thực hiện trên cơ sở xem xét mức độ chịu đựng của cơ quan/tổ chức với các rủi ro tiếp diễn. Cần xác định, đánh giá và ghi nhận các yếu tố liên quan như

- Các lỗ hổng với các tài nguyên và hoạt động nhạy cảm với thời gian
- Các đe dọa và mối nguy với tài nguyên và hoạt động khẩn cấp nhất
- Đo lường mức độ, khả năng hay hậu quả của việc gián đoạn các dịch vụ và sản phẩm then chốt.

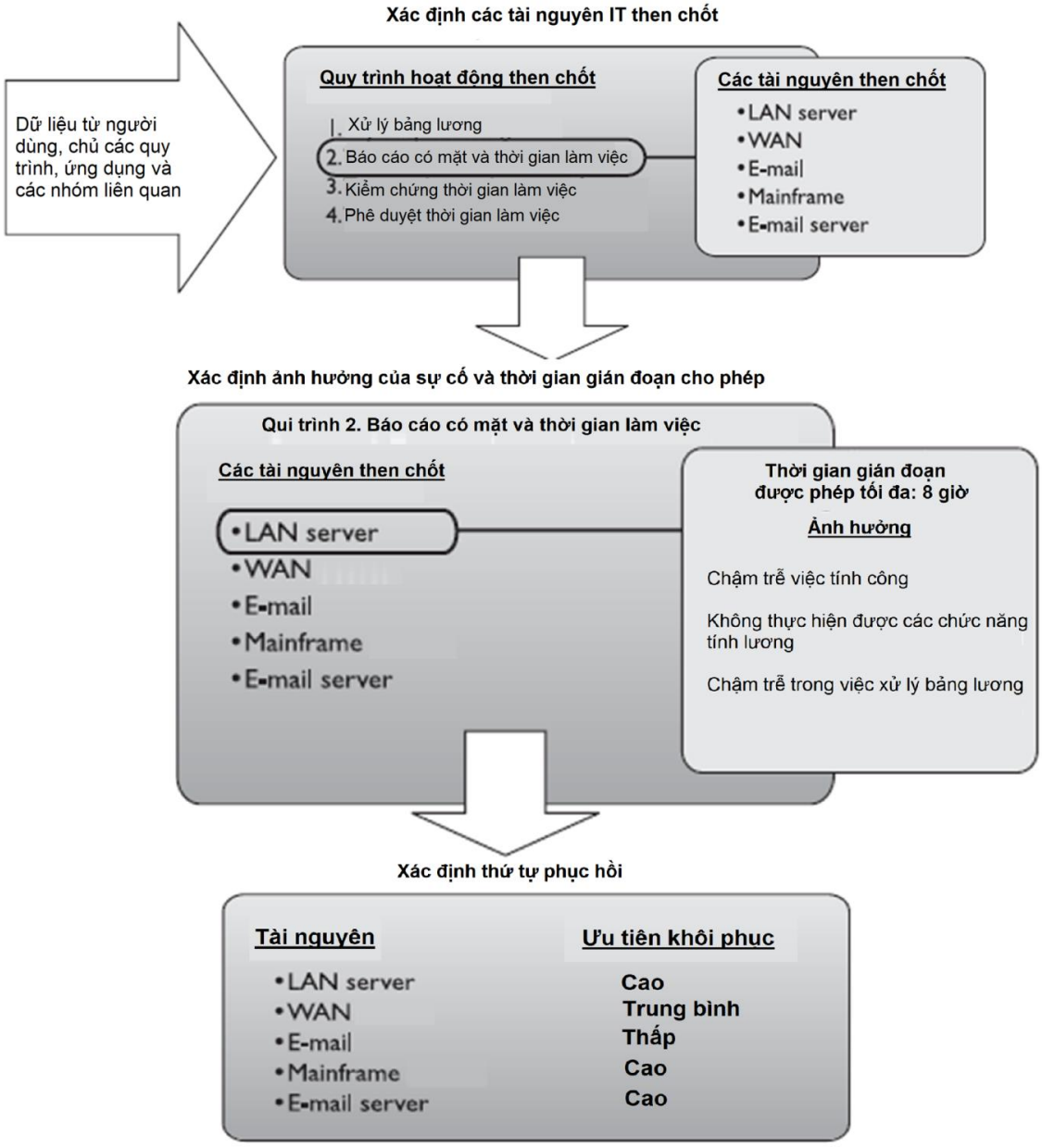
- Các nút cổ chai hay mức độ tập trung rủi ro đe dọa hoạt động liên tục
- Rủi ro do việc tập trung kỹ năng hay khan hiếm kỹ năng then chốt
- Rủi ro do các nhà cung cấp bên ngoài.

Các chú ý các yếu tố tác động không đo đếm trực tiếp về mặt tài chính

- Làm nản lòng khách hàng
- Mất nhân viên do công việc bị đình trệ quá lâu
- Ảnh hưởng tiêu cực của cộng đồng

Mức độ rủi ro được đánh giá theo công thức

*Rủi ro = f(Đe dọa, Tác động, Mức độ chắc chắn)*




**Hình 6-4. Đánh giá các tài nguyên cần thiết.**

### 6.2.3 *Lập kế hoạch duy trì*

Giai đoạn tiếp theo của xây dựng kế hoạch duy trì hoạt động tập trung vào việc phát triển và thực hiện một chiến lược duy trì hoạt động để giảm thiểu các rủi ro có thể có đối với tài sản được bảo vệ. Việc xây dựng chiến lược duy trì thu hẹp khoảng cách giữa đánh giá tác động và các giai đoạn lập kế hoạch duy trì trong việc xây dựng kế hoạch duy trì hoạt động. Nhóm xây dựng kế hoạch giờ đây phải đưa ra danh sách các mối quan tâm được ưu tiên thông qua việc đánh giá và phân tích tác động và xác định những rủi ro nào sẽ được giải quyết bằng kế hoạch duy trì hoạt động. Giải quyết tất cả các trường hợp bất thường sẽ cần thực hiện các quy định và quy trình để đảm bảo không có thời gian dừng khi đối mặt với mọi rủi ro có thể xảy ra. Rõ ràng, việc triển khai chính sách toàn diện kiểu này đơn giản là không thể.

Nhóm lập kế hoạch nên xem xét lại các ước tính về thời gian gián đoạn chịu đựng được trong giai đoạn đầu của việc đánh giá tác động và xác định những rủi ro nào được coi là chấp nhận được và phải được giảm thiểu bởi các quy định duy trì hoạt động. Khi nhóm lập kế hoạch xác định những rủi ro nào cần giảm thiểu và mức độ tài nguyên sẽ được cam kết cho mỗi nhiệm vụ giảm thiểu, nhóm sẵn sàng chuyển sang xây dựng các quy định và quy trình của giai đoạn lập kế hoạch liên tục.

Các quy định và quy trình của giai đoạn lập kế hoạch duy trì hoạt động là cốt lõi của toàn bộ kế hoạch. Nhóm lập kế hoạch thiết kế các quy trình và cơ chế cụ thể nhằm giảm thiểu các rủi ro được coi là không thể chấp nhận được trong giai đoạn xây dựng chiến lược. Ba loại tài sản phải được bảo vệ thông qua các quy định và quy trình là con người, phương tiện và cơ sở hạ tầng.

Trước hết, kế hoạch phải đảm bảo rằng những người trong cơ quan/tổ chức được an toàn trước trong và sau khi tình huống khẩn cấp. Khi đã đạt được mục tiêu này, nhóm lập kế hoạch thực hiện các điều khoản để cho phép nhân viên thực hiện kế hoạch duy trì và công việc của họ theo cách thông thường theo hoàn cảnh. Thực tế rằng con người là tài sản quý giá nhất của cơ quan/tổ chức. Sự an toàn của con người phải luôn luôn đi trước các mục tiêu hoạt động của cơ quan/tổ chức. Cần đảm bảo rằng kế hoạch duy trì hoạt động đưa ra các quy định đầy đủ về bảo đảm an ninh nhân viên, khách hàng, nhà cung cấp và bất kỳ cá nhân nào khác có thể bị ảnh hưởng.

Nhiều cơ quan/tổ chức yêu cầu các cơ sở và phương tiện chuyên môn để thực hiện các hoạt động quan trọng của mình. Đây có thể bao gồm các cơ sở văn phòng tiêu chuẩn, nhà máy sản xuất, trung tâm hoạt động, kho, trung tâm phân phối / hậu cần, và kho sửa chữa/bảo trì. Khi thực hiện đánh giá tác động cần xác định những cơ sở/phương tiện đóng vai trò quan trọng trong khả năng tồn tại liên tục của cơ quan/tổ chức.

Mặt khác, mỗi cơ quan/tổ chức phụ thuộc vào một số loại cơ sở hạ tầng cho các quy trình quan trọng. Một phần quan trọng của cơ sở hạ tầng này hệ thống xương sống CNTT về truyền thông và máy tính xử lý đơn đặt hàng, quản lý chuỗi cung ứng, xử lý tương tác của khách hàng và thực hiện các chức năng hoạt động khác. Hệ thống xương sống này

bao gồm một số máy chủ, máy trạm và các liên kết truyền thông quan trọng giữa các trang web. Kế hoạch duy trì hoạt động phải giải quyết biện pháp bảo vệ các hệ thống này sẽ khỏi các rủi ro.

### 6.2.4 *Phê chuẩn và triển khai*

Khi nhóm xây dựng kế hoạch duy trì hoạt động hoàn thành giai đoạn thiết kế của tài liệu của việc lập kế hoạch cần đạt được việc phê chuẩn của quản lý cấp cao nhất về kế hoạch này. Nếu có được sự tham gia quản lý cấp cao trong suốt các giai đoạn xây dựng của kế hoạch hoạt động thì đây sẽ là một quá trình tương đối đơn giản. Mặt khác, nếu đây là lần đầu tiên ban quản lý cấp cao tiếp cận các tài liệu của kế hoạch hoạt động này, nhóm xây dựng kế hoạch cần sẵn sàng để giải thích chi tiết về mục đích của chương trình và các điều khoản cụ thể. Việc quản lý cấp cao tin tưởng và phê duyệt là cần thiết cho sự thành công của kế hoạch duy trì hoạt động. Việc xác nhận bởi các lãnh đạo cấp cao thể hiện tầm quan trọng của kế hoạch đối với toàn bộ tổ chức và thể hiện cam kết của ban lãnh đạo đối với duy trì hoạt động của cơ quan/tổ chức.

Sau khi nhận được sự chấp thuận của ban quản lý cấp cao, đã đến lúc tìm hiểu và bắt đầu triển khai kế hoạch duy trì hoạt động. Nhóm xây dựng kế hoạch phát triển lịch trình triển khai sử dụng các nguồn lực dành riêng cho chương trình để đạt được các kết quả theo các quy trình và điều khoản đề ra một cách nhanh nhất. Sau khi tất cả các tài nguyên được triển khai đầy đủ, nhóm nên giám sát việc thực hiện các chương trình duy trì hoạt động một cách thích hợp để đảm bảo rằng kế hoạch vẫn đáp ứng nhu cầu hoạt động và phát triển.

Bên cạnh đó, đào tạo và giáo dục là những yếu tố thiết yếu của việc thực hiện kế hoạch duy trì hoạt động. Tất cả nhân viên sẽ tham gia vào kế hoạch (trực tiếp hoặc gián tiếp) sẽ nhận được một số dạng đào tạo về kế hoạch tổng thể và trách nhiệm cá nhân của họ. Mọi người trong tổ chức sẽ nhận được ít nhất một bản tóm tắt về kế hoạch duy trì hoạt động để đảm bảo cho họ niềm tin rằng các lãnh đạo đã xem xét những rủi ro có thể xảy ra với việc duy trì hoạt động của cơ quan/tổ chức và đã lên kế hoạch để giảm thiểu tác động đối với cơ quan/tổ chức khi xảy ra sự cố hay thảm họa.

Những người có trách nhiệm trực tiếp về kế hoạch duy trì hoạt động cần được đào tạo và đánh giá về các nhiệm vụ cụ thể của họ để đảm bảo rằng họ có thể hoàn thành kế hoạch này một cách hiệu quả khi thảm họa xảy ra. Hơn nữa, ít nhất cần một người dự phòng nên được huấn luyện cho mọi nhiệm vụ kế hoạch duy trì hoạt động để đảm bảo sự sẵn sàng khi các nhân sự bị thương hoặc không thể đến nơi làm việc trong trường hợp khẩn cấp.

## 6.3 Chiến lược khôi phục sự cố

Trong giai đoạn chiến lược khôi phục, nhóm xây dựng tiếp cận thông tin thu thập được trong giai đoạn phân tích hoạt động của cơ quan/tổ chức từ góc độ thực tế. Điều cần

phải tìm ra những gì cơ quan/tổ chức cần làm để thực sự phục hồi các mục được xác định là rất quan trọng đối với cơ quan/tổ chức nói chung. Trong chiến lược duy trì và phục hồi hoạt động của mình, nhóm xây dựng thẩm tra chặt chẽ các chức năng hoạt động quan trọng và được chấp thuận. Sau đó đánh giá nhiều phương án khôi phục và sao lưu có thể được sử dụng để phục hồi việc thực hiện của các hoạt động quan trọng. Điều quan trọng là chọn chiến thuật và công nghệ phù hợp cho việc khôi phục các quy trình hoạt động và dịch vụ thiết yếu để đảm bảo thời gian gián đoạn chấp nhận được.

Nhóm xây dựng cần xác định các chiến lược phục hồi, thực tế là một tập hợp các hoạt động được xác định trước sẽ được triển khai và thực hiện để ứng phó với thảm họa. Các chiến lược khôi phục này thành các phần sau:

- Khôi phục quy trình hoạt động
- Khôi phục phương tiện
- Khôi phục nguồn cung cấp và công nghệ
- Khôi phục môi trường người dùng
- Khôi phục dữ liệu

Phần dưới đây trình bày chiến lược khôi phục với 3 mục đầu.

### 6.3.1 *Khôi phục quy trình hoạt động*

Quy trình hoạt động là tập các bước liên kết với nhau theo các hành động cụ thể để hoàn thành nhiệm vụ/công việc. Nhóm lập kế hoạch hoạt động cần phải nắm bắt chi tiết về các quy trình thiết yếu của cơ quan/tổ chức như dữ liệu mô tả các vai trò nguồn lực cần cho các quy trình này:

- Vai trò và tài nguyên cần thiết
- Đầu vào và ra
- Các bước trong luồng công việc
- Thời gian cần hoàn thành
- Giao diện với các quy trình khác

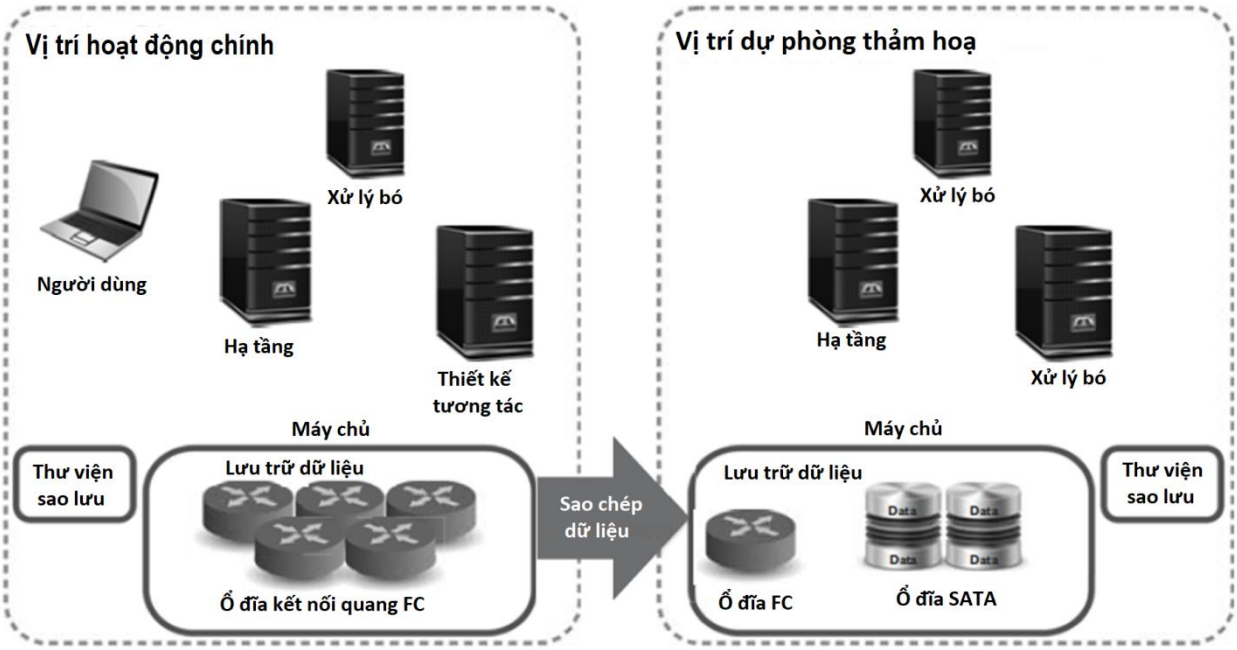
Các thông tin này giúp cho nhóm xác định các mối đe dọa và biện pháp kiểm soát để giảm thiểu thời gian gián đoạn.

### 6.3.2 *Khôi phục phương tiện*

Việc gián đoạn hoạt động có thể xếp vào 3 dạng: thông thường, thảm họa, thảm họa nghiêm trọng. Với gián đoạn thông thường, chiến lược khôi phục là thay thế hay sửa chữa các trang thiết bị, phần cứng hay phần mềm. Với thảm họa thường do nguyên nhân thiên nhiên như bão tố, ngập lụt, thời gian gián đoạn tính bằng ngày hoặc lâu hơn. Việc khôi phục phải dựa vào các trang thiết bị hay phương tiện từ vị trí khác. Thông thường cần các trang thiết bị sẵn sàng thay thế cho thiết bị/phương tiện bị gián đoạn từ vị khác với vị trí bị thảm họa. Hình 6-5 mô tả cấu hình tiêu biểu và cách sao lưu dữ liệu giữa các vị trí hoạt động và dự phòng.

Thảm họa nghiêm trọng gây ra sự gián đoạn trầm trọng với phương tiện và trang thiết bị, có thể phá hủy hoàn toàn các phương tiện hiện có. Việc khôi phục cần cả biện pháp ngắn và dài hạn:

- Ngắn hạn: sử dụng các thiết bị trợ giúp từ vị trí khác
- Dài hạn: xây dựng và sửa chữa lại phương tiện như phòng ốc hay nhà xưởng




**Hình 6-5. Vị trí hoạt động và dự phòng.**

Cơ quan/tổ chức có một số lựa chọn để đối phó với các nguyên nhân gây gián đoạn trên cơ sở cân nhắc lợi ích/chi phí:

- Xây dựng vị trí dự phòng
- Thuê ngoài (outsource)
- Thuê vị trí dự phòng

Khi thuê phương tiện dự phòng, cơ quan/tổ chức đi thuê cần cân nhắc

- Mức độ tin cậy bên được thuê
- Khả năng sẵn dùng của các phương tiện được thuê dự phòng
- Chia sẻ phương tiện dự phòng/ứng cứu với cơ quan/tổ chức liên quan

### 6.3.3 *Khôi phục nguồn cung cấp và công nghệ*

Nhóm quản lý cần xác định các chi tiết giải pháp dự phòng cho

- Các thiết bị máy tính và mạng
- Các tài nguyên liên lạc cho dữ liệu và thoại
- Nhân lực
- Vận chuyển thiết bị và con người
- Các vấn đề an toàn cho dữ liệu và con người
- Nguồn cung cấp

Môi trường kỹ thuật hiện tại của cơ quan/tổ chức phải được hiểu rõ. Điều này có nghĩa là nhóm lập kế hoạch phải biết các chi tiết cụ thể của mạng, công nghệ truyền thông, máy tính, thiết bị mạng và các yêu cầu phần mềm mà cần thiết để các chức năng thiết yếu hoạt động được. Thực tế các yếu tố này thay đổi theo thời gian và cần cập nhật một cách kịp thời để khi môi trường hoạt động của cơ quan/tổ chức bị gián đoạn hay phá hủy thì nhóm khôi phục có đủ thông tin và kỹ năng cần thiết để xây dựng lại một cách thích đáng.

## 6.4 Kiểm thử và cập nhật kế hoạch

Khi hoàn thành các chiến lược khôi phục, nhóm lập kế hoạch cần chuyển các chiến lược này vào trạng thái sẵn sàng. Nói cách khác, khi này cần chuyển từ giai đoạn lập kế hoạch thuần túy sang giai đoạn thực hiện và hành động thực tế.

Các bản sao của các kế hoạch thực hiện cần phải được lưu giữ tại một hoặc nhiều vị trí khác với trang web chính, để nếu vị trí chính bị phá hủy hoặc bị ảnh hưởng tiêu cực, kế hoạch liên tục vẫn có sẵn cho các nhóm. Điều cũng quan trọng là các định dạng khác nhau của kế hoạch có sẵn cho nhóm, bao gồm cả phiên bản điện tử và giấy. Phiên bản điện tử không hữu ích lắm nếu không có điện để máy tính hoạt động.

Kế hoạch nên đề cập tất cả các chi tiết theo chủ đề. Định dạng thực tế của kế hoạch sẽ phụ thuộc vào môi trường, mục tiêu của kế hoạch, ưu tiên và các mối đe dọa đã xác định. Sau mỗi mục được kiểm tra và ghi lại, các chủ đề của kế hoạch có thể được chia thành các loại cần thiết. Bảng dưới đây liệt kê các kế hoạch tiêu biểu cho việc khôi phục. Tùy thuộc vào các thức quản lý và nhóm xây dựng kế hoạch để xác định số lượng và các dạng kế hoạch cần được phát triển và triển khai.

**Bảng 6-1. Các kiểu kế hoạch khôi phục.**

| Kiểu kế hoạch | Mục tiêu |
|---|---|
| Kế hoạch khôi phục hoạt động | Tập trung vào việc khởi tạo lại các quy trình hoạt động cần thiết để hoạt động lại thay vì tập trung vào thiết bị CNTT |
| Tính liên tục của các kế hoạch hành động | Thiết lập quản lý cấp cao và trung tâm xử lý ngay khi có thảm họa (sự cố). Vạch ra các chức trách và vai trò, thứ tự hành động, và nhiệm vụ của từng cá nhân |
| Kế hoạch cho tính liên tục của CNTT | Kế hoạch cho các thủ tục/quy trình khôi phục hệ thống, mạng và ứng dụng sau khi thảm họa. Cần các các quy trình/thủ tục cho từng bộ phận quan trọng/chủ yếu |
| Kế hoạch truyền | Bao gồm các vai trò và cơ chế truyền thông nội bộ và bên |

| | |
|---|---|
| thông khủng hoảng | ngoài. Xác định các cá nhân cụ thể sẽ liên lạc với bên ngoài. Bao gồm các phát biểu được chuẩn bị trước mà cần được công bố |
| Kế hoạch đối phó sự cố mạng | Tập trung vào phần mềm độc hại, xâm nhập, tấn công, và các vấn đề an toàn khác. Vạch ra các thủ tục để đối phó với sự cố |
| Kế hoạch khẩn cấp (với nhân viên) | Xây dựng an toàn lao động và thủ tục sơ tán |

### 6.4.1 *Kiểm thử kế hoạch*

Các kế hoạch cần phải được kiểm thử thường xuyên do môi trường hoạt động của cơ quan/tổ chức liên tục thay đổi. Để giảm thái độ thiếu hợp tác trong việc kiểm thử, người quản lý có thể coi việc kiểm thử như là việc thực hành thường xuyên các kế hoạch để đánh giá, cải thiện và nâng hiệu quả của các kế hoạch.

Việc kiểm thử/thực hành giúp cho mọi người (nhân viên/lãnh đạo) làm quen với các tình huống và nhiệm vụ họ phải đối mặt và giải quyết trong môi trường có kiểm soát.Các bài kiểm tra và thực hành khôi phục và khắc phục thảm họa nên được thực hiện ít nhất mỗi năm một lần. Cơ quan/tổ chức thực sự không có sự tự tin khi xây dựng kế hoạch cho đến khi kế hoạch này đã thực sự được thử nghiệm. Các bài kiểm tra và diễn tập chuẩn bị nhân sự cho những gì họ có thể phải đối mặt và cung cấp một môi trường được kiểm soát để tìm hiểu các nhiệm vụ dự kiến của họ. Các bài kiểm tra và diễn tập này cũng chỉ ra các vấn đề đối với nhóm lập kế hoạch và quản lý mà trước đó có thể chưa được suy nghĩ và giải quyết như là một phần của quy trình lập kế hoạch. Các bài tập, cuối cùng, chứng minh tổ chức thực sự có thể phục hồi sau một thảm họa.

Diễn tập phải có một kịch bản được xác định trước mà cơ quan/tổ chức thực sự có thể phải đối mặt với trong một thời điểm nào đó. Các thông số cụ thể và phạm vi của diễn tập phải được chỉ ra trước khi cảnh báo sự cố. Nhóm thực hành diễn tập phải chấp thuận một cách chính xác những gì đang được thử nghiệm và cách xác định thành công hay thất bại. Ngoài ra, nhóm cần xác định xem phần cứng, phần mềm, nhân sự, quy trình và các tuyến liên lạc được kiểm tra. Nếu diễn tập bao gồm việc di chuyển một số thiết bị đến một địa điểm thay thế thì việc vận chuyển, trang thiết bị phụ và sự sẵn sàng vị trí thay thế phải được giải quyết và đánh giá.

Cần xác định các chi phí liên quan đến việc thử/thực hành bao gồm:

- Thời điểm và khoảng thời gian
- Quy trình, nhân lực, phương tiện liên lạc
- Các phương tiện phần cứng, phần mềm cần thiết

- Phương tiện vận chuyển, vị trí thử nghiệm/thực hành

Những người thực hiện các cuộc diễn tập này nói chung sẽ gặp các vấn đề và mắc sai lầm. Đây là lý do cần có các cuộc diễn tập và thử nghiệm để tất cả mọi người có thể học hỏi và thực hiện nhiệm vụ của mình hiệu quả hơn khi xảy ra thảm họa thực sự.

### 6.4.2 *Các dạng kiểm thử*

Phần dưới đây trình bày các dạng kiểm thử tiêu biểu nên được tiến hành để nâng cao hiệu quả khắc phục sự cố duy trì hoạt động của cơ quan/tổ chức.

a. *Kiểm thử đầu mục*

- Các bản sao kế hoạch đảm bảo duy trì hoạt động được gửi cho các phòng ban chức năng để đánh giá lại.
- Mục tiêu là không để sót bất kỳ mục nào trong kế hoạch dự phòng tại bất kỳ phòng ban chức năng nào.

b. *Kiểm tra cấu trúc vắn tắt*

- Đại diện của các phòng ban cùng nhau duyệt qua các kế hoạch để đảm bảo tính chính xác của chúng
- Các nội dung thảo luận bao gồm các phạm vi, quy mô, giả định của kế hoạch, đánh giá lại cấu trúc quản lý, điều hành cũng như các yêu cầu cho việc đào tạo, duy trì và kiểm thử

c. *Kiểm thử giả lập*

- Tất cả nhân viên tham gia vào việc vận hành hay hỗ trợ hoạt động của cơ quan/tổ chức, hay đại diện của họ cùng thực hành các kế hoạch phục hồi thảm họa dựa trên các tình huống cụ thể.
- Cho phép kiểm tra phản ứng của các đại diện/nhân viên các phòng ban khi xử lý sự cố.
- Đảm bảo không bỏ sót bước nào trong kế hoạch dự phòng cũng như các mối đe dọa đều không bị coi thường .

d. *Kiểm thử song song*

- Việc kiểm thử nhằm đánh giá các hệ thống dự phòng ở vị trí khác hoạt động một cách thích đáng.
- Kết quả được so sánh với việc vận hành của hệ thống bình thường để đánh giá lại việc cấu hình cũng như quy trình và sửa đổi cần thiết.

e. *Kiểm thử gián đoạn hoàn chỉnh*

- Thử nghiệm này ảnh hưởng nghiêm trọng đến việc vận hành bình thường cũng như năng suất hoạt động của cơ quan/tổ chức.

- Toàn bộ hệ thống hiện thời sẽ bị ngắt và thực hiện việc chuyển sang vị trí dự phòng.
- Nhóm khôi phục thực hiện đầy đủ việc chuẩn bị hệ thống cũng như môi trường hoạt động ở vị trí mới.
- Việc diễn tập này giúp phát hiện các lỗ hổng trong kế hoạch
- Việc kiểm thử này chỉ thực hiện sau khi các phép thử khác đã thành công và sau khi được phê duyệt của ban lãnh đạo cấp cao.

### 6.4.3 *Cập nhật kế hoạch*

Việc thiếu cập nhật kế hoạch làm cho mọi người không nắm được thực tế và yêu cầu mới về an toàn. Các yếu tố ảnh hưởng khiến cho kế hoạch dự phòng nhanh chóng lỗi thời:

- Các quy trình đảm bảo duy trì hoạt động không được tích hợp với việc thay đổi quy trình quản lý
- Tái cấu trúc/tổ chức lại cơ quan
- Thay đổi về công nghệ (phần cứng/phần mềm)
- Di chuyển nhân sự
- Tốn công sức cho việc cập nhật kế hoạch
- Kế hoạch không trực tiếp mang lại lợi nhuận

Các hành động cần thiết cho việc đảm bảo cập nhật:

- Đảm bảo yêu cầu duy trì hoạt động là một phần của mỗi quyết định hoạt động/kinh doanh
- Yêu cầu trách nhiệm cập nhật rõ ràng trong mô tả công việc
- Làm một phần trong việc đánh giá hiệu quả của mỗi cá nhân
- Thực hiện việc kiểm tra/kiểm toán về việc cập nhật
- Thực hiện việc thực hành thường xuyên
- Tích hợp các kế hoạch dự phòng vào quy trình quản lý sự thay đổi
- Liên kết các bài học thực tế từ các sự cố vào trong kế hoạch

Một trong những cách đơn giản, tiết kiệm chi phí và hiệu quả nhất để giữ kế hoạch được cập nhật là kết hợp nó trong quy trình quản lý thay đổi. Quy trình quản lý thay đổi phải được cập nhật để kết hợp các trường và trình kích hoạt cảnh báo nhóm lập kế hoạch duy trì hoạt động và khi có thay đổi đáng kể sẽ cung cấp phương tiện để cập nhật tài liệu khôi phục.

## 6.5 Câu hỏi ôn tập

1. Trình bày sự khác biệt giữa kế hoạch khôi phục sự cố và hoạt động liên tục.
2. Giải thích vấn đề khôi phục quy trình hoạt động.
3. Nêu các vấn đề khôi phục trang thiết bị.
4. Trình bày vấn đề khôi phục nguồn cung cấp và công nghệ.
5. Trình bày mục tiêu của việc kiểm tra/thực hành các kế hoạch đảm bảo hoạt động liên tục.
6. Giải thích mục tiêu và yêu cầu của các dạng kiểm thử.
7. Phân tích các yêu cầu đảm bảo hoạt động liên tục của một quy trình sản xuất tùy chọn như xử lý đơn hàng?
8. Phân tích yêu cầu đảm bảo hoạt động liên tục cho quá trình lựa chọn các sản phẩm khi mua hàng trực tuyến.

# CHƯƠNG 7. CHÍNH SÁCH VÀ PHÁP LUẬT AN TOÀN THÔNG TIN

Mục tiêu của chương này trình bày các yêu cầu cơ bản về các chính sách an toàn thông tin của cơ quan hay tổ chức. Các chính sách an toàn này một mặt thể hiện mục tiêu mà cơ quan hay tổ chức đó cần đạt được, mặt khác chúng chứng tỏ sự tuân thủ với các quy định pháp luật cũng như sự đóng góp với xã hội và đối tác về việc đảm bảo an toàn thông tin. Phần tiếp theo của chương giới thiệu các ràng buộc về mặt pháp lý cũng như các hoạt động trong lĩnh vực thông tin và liên lạc của cá nhân và tổ chức cần phải tuân thủ trên lãnh thổ Việt Nam. Phần còn lại của chương giới thiệu các luật quan trọng liên quan đến vấn đề bảo vệ thông tin trong môi trường mạng của các nước Châu Âu, Mỹ và một số quốc gia trong khu vực.

## 7.1 Các yêu cầu về chính sách, pháp luật

### 7.1.1 *Giới thiệu*

Trong cơ quan/tổ chức, các hệ thống máy tính và cách thức xử lý thông tin có mối quan hệ trực tiếp và then chốt với các nhiệm vụ và mục tiêu quan trọng của cơ quan/tổ chức trong quá trình hoạt động. Do tầm quan trọng này, quản lý cấp cao cần bảo vệ các yếu tố này với mức ưu tiên cao và dành sự hỗ trợ, tài chính, thời gian và tài nguyên cần thiết để đảm bảo rằng hệ thống, mạng và thông tin phục vụ cho công việc được bảo vệ theo cách hợp lý và hiệu quả nhất có thể.

Để kế hoạch an toàn thành công, kế hoạch này phải bắt đầu ở cấp cao nhất cũng như có ích và hiệu lực ở mọi cấp độ. Quản lý cấp cao cần xác định phạm vi an toàn và xác định những gì phải được bảo vệ và ở mức độ nào. Đội ngũ lãnh đạo phải nắm các quy định, luật pháp và các vấn đề trách nhiệm pháp lý cũng như chịu trách nhiệm tuân thủ các ràng buộc liên quan đến an toàn. Bên cạnh đó, ban lãnh đạo đảm bảo rằng cơ quan/tổ chức chấp hành đầy đủ nghĩa vụ của mình cũng như xác định những điều mong đợi từ nhân viên và hậu quả của việc không tuân thủ. Những quyết định này nên được thực hiện bởi những cá nhân chịu trách nhiệm cuối cùng khi việc vi phạm xảy ra. Thực tế phổ biến cho thấy, để đạt được các mục tiêu do quản lý cấp cao thiết lập và xác định cần kiến thức chuyên môn của các nhân viên phụ trách an toàn trong việc phối hợp và đảm bảo rằng các chính sách và biện pháp kiểm soát phù hợp được thực hiện.

### 7.1.2 *Các yêu cầu của chính sách*

Chính sách an toàn là một tuyên bố chung khái quát được quản lý cấp cao đưa ra trong đó xác định các vai trò an toàn trong cơ quan/tổ chức được thực hiện như thế nào. Chính sách an toàn có thể là quy tắc tổ chức; chính sách dành riêng cho vấn đề cụ thể hay cho hệ thống. Trong chính sách an toàn của cơ quan/tổ chức, đội ngũ quản lý xác định

cách thức thiết lập chương trình an toàn, đưa ra các mục tiêu của chương trình, phân công trách nhiệm, vạch ra các giá trị ngắn hạn và dài hạn về an toàn cũng như cách thực thi. Chính sách này phải giải quyết các luật, quy định và các vấn đề trách nhiệm pháp lý tương đối và cách chúng được chấp hành. Chính sách an toàn của cơ quan/tổ chức xác định phạm vi và hướng cho tất cả các hoạt động đảm bảo an toàn trong tương lai trong cơ quan/tổ chức. Chính sách an toàn cũng mô tả mức độ rủi ro mà quản lý cấp cao sẵn sàng chấp nhận.

Các dạng cơ bản của chính sách có thể bao gồm:

- Quy định đảm bảo rằng cơ quan/tổ chức tuân theo các tiêu chuẩn được thiết lập bởi các quy định ngành cụ thể. Chúng rất chi tiết và cụ thể cho một loại ngành. Các quy định có thể được sử dụng trong các tổ chức tài chính, cơ sở chăm sóc sức khỏe, tiện ích công cộng và các ngành khác do chính phủ quản lý.
- Tư vấn/Khuyến nghị nhằm khuyến khích một cách mạnh mẽ cho nhân viên về các hành vi và hoạt động nào nên và không nên diễn ra trong cơ quan/tổ chức. Các chính sách này cũng vạch ra các trường hợp có thể khi nhân viên không tuân thủ các hành vi và hoạt động đã thiết lập.
- Thông tin nhằm thông báo cho nhân viên về các vấn đề nhất định và thường là các hướng dẫn cá nhân về các vấn đề cụ thể liên quan đến cơ quan/tổ chức. Các chính sách này giải thích cách cơ quan/tổ chức tương tác với các đối tác, các mục tiêu và nhiệm vụ và cấu trúc báo cáo chung trong các tình huống khác nhau.

Các lĩnh vực cơ bản mà chính sách đề cập đến gồm có:

- Chính sách sử dụng được chấp nhận
- Chính sách quản lý rủi ro
- Chính sách quản lý lỗ hổng
- Chính sách bảo vệ dữ liệu
- Chính sách kiểm soát truy cập
- Chính sách duy trì hoạt động
- Chính sách thu thập log và kiểm toán
- Chính sách an toàn nhân sự
- Chính sách kiểm soát thay đổi
- Chính sách ứng phó sự cố

Các yêu cầu cơ bản cho việc thực hiện đầy đủ và thành công các mục tiêu an toàn của chính sách đó là:

- Phổ biến (phân phát): Mọi người trong cơ quan/tổ chức đều có thể đọc và xem xét các chính sách phù hợp.

- Đánh giá (đọc): Cơ quan/tổ chức cần phân phát các tài liệu theo dạng dễ hiểu dễ đọc cho mọi đối tượng nhân viên như tài liệu bằng nhiều ngôn ngữ
- Nhận thức (hiểu): Mỗi nhân viên đều hiểu các yêu cầu và nội dung của các chính sách
- Chấp thuận (đồng ý): Đảm bảo các nhân viên đồng ý tuân thủ chính sách bằng hành động hay xác nhận
- Thi hành nhất quán: Cơ quan/tổ chức cần đảm bảo chính sách được thực thi nhất quán bất kể tình trạng hay công việc của nhân viên

### 7.1.3 *Chính sách, tiêu chuẩn và luật pháp*

Các tiêu chuẩn đề cập đến các hoạt động, hành động hoặc quy tắc bắt buộc. Chúng có thể là một quy trình hoặc một cách thức để thực hiện một giải pháp. Điều này liên quan đến công nghệ, phần cứng hoặc phần mềm đã có mà đã được chứng minh về hiệu quả. Đây có thể là một quy định hay hướng dẫn kỹ thuật thực thi được triển khai trên toàn cơ quan/tổ chức. Tiêu chuẩn đảm bảo an toàn của cơ quan/tổ chức có thể chỉ định cách sử dụng các sản phẩm phần cứng và phần mềm. Tiêu chuẩn cũng có thể được sử dụng để xác định hành vi người dùng mong đợi. Như vậy, các tiêu chuẩn cung cấp phương tiện để đảm bảo rằng các công nghệ, ứng dụng, thông số và quy trình cụ thể được thực hiện theo cách thống nhất (chuẩn) trên toàn tổ chức.

Với các mục tiêu của an toàn thông tin, các tiêu chuẩn là tập các tiêu chí mà hệ thống thông tin phải thực hiện. Cơ quan/tổ chức có thể có các tiêu chuẩn nội bộ của mình. Thông thường các tiêu chuẩn này được điều chỉnh cho phù hợp dựa trên một số thực tiễn tốt nhất từ bên ngoài. Việc áp dụng tiêu chuẩn phù hợp đảm bảo rằng các bài học kinh nghiệm đã được xem xét.

Chính sách của cơ quan/tổ chức triển khai các biện pháp kiểm soát trên hệ thống để làm cho nó đáp ứng tiêu chuẩn nào đó. Các tiêu chuẩn hỗ trợ và định hướng cho việc xây dựng chính sách. Tiêu chuẩn thường xác định yêu cầu tối thiểu nhưng có thể rất chi tiết về bản chất. Thực tế, quy định pháp luật hoặc thực tiễn đã được chấp thuận rộng rãi tạo ra các tiêu chuẩn. Sau đó, các tiêu chuẩn này trở thành tiêu chí cho quản trị hoặc chứng nhận và công nhận.

Tiêu chuẩn thường bắt đầu với các tiêu chuẩn công nghiệp. Theo thời gian, các tổ chức đại diện cho ngành công nghiệp phát triển và xuất bản các tiêu chuẩn. Những tiêu chuẩn này thường trở thành thước đo mà theo đó các nhà quản lý đánh giá các cơ quan/tổ chức. Cần phải cẩn trọng khi lệch quá xa các tiêu chuẩn của ngành. Việc không tuân thủ chúng có thể dẫn đến các hình phạt dân sự và pháp lý. Ví dụ như tiêu chuẩn bảo mật dữ liệu thẻ thanh toán (PCI DSS) có thể áp dụng mức phạt lên tới 50.000$ /ngày cho việc vi phạm tiêu chuẩn đã công bố hay 500.000$ cho mỗi sự vụ liên quan đến an toàn dữ liệu.

Ở góc độ xã hội, các hoạt động CNTT ảnh hưởng tới nhiều đối tượng cũng như lĩnh vực khác nhau nên chịu sự tác động của nhiều luật nhằm xác định và điều chỉnh cách hành vi cũng như kiểm soát việc truy nhập và sử dụng thông tin như:

- Sử dụng, trao đổi và phân phát dữ liệu
- Sử dụng máy tính cho việc xử lý, trao đổi dữ liệu
- Thông tin cá nhân
- Thông tin của tổ chức, cơ quan nhà nước
- Thương mại điện tử
- Ngân hàng điện tử
- Bản quyền
- Khủng bố và chống khủng bố

Các hoạt động của cơ quan/tổ chức cũng như các chính sách và tiêu chuẩn áp dụng cần pháp đáp ứng và tuân thủ một cách đầy đủ các quy định về luật pháp tác động lên cơ quan/tổ chức đó. Việc không chấp hành một cách đầy đủ các quy định này có thể dẫn đến các hậu quả rất nghiêm trọng từ phạt tiền đến gián đoạn việc hoạt động và thậm chí chấm dứt hoạt động của cơ quan/tổ chức.

## 7.2 Các luật về an toàn thông tin của Việt Nam

### 7.2.1 *Các văn bản pháp luật*

Các văn bản pháp luật do quốc hội Việt Nam ban hành (Luật 80/2015/QH13):

1. Hiến pháp: có hiệu lực pháp lý cao nhất và quy định những vấn đề cơ bản của quốc gia
2. Bộ luật, luật: nhằm mục đích cụ thể hóa hiến pháp điều chỉnh các quan hệ xã hội trong các lĩnh vực đời sống nhà nước và xã hội.

Các văn bản dưới luật do các cơ quan có thẩm quyền ban hành và có hiệu lực pháp lý thấp hơn:

1. Pháp lệnh, nghị quyết của Ủy ban thường vụ Quốc hội;
2. Lệnh, quyết định của Chủ tịch nước.
3. Nghị định của Chính phủ; Quyết định của Thủ tướng Chính phủ.
4. Thông tư (thông tư liên tịch) của Bộ trưởng, Thủ trưởng cơ quan ngang bộ;

Bảng 7-1 dưới đây liệt kê các văn bản pháp luật đã được ban hành về lĩnh vực liên quan an toàn thông tin.

**Bảng 7-1. Các văn bản pháp luật về an toàn thông tin**

| Số hiệu | Hình thức | Lĩnh vực | Trích yếu nội dung |
|---|---|---|---|
| 24/ 2018/ QH14 | Luật | An ninh mạng | Quy định về hoạt động bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội trên không gian mạng; trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan. |
| 632/ QĐ-TTg | Quyết định | CNTT, điện tử, An toàn thông tin | Ban hành danh mục lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng và hệ thống thông tin quan trọng quốc gia |
| 85/ 2016/ NĐ-CP | Nghị định | CNTT, điện tử | Về bảo đảm an toàn hệ thống thông tin theo cấp độ |
| 108/ 2016/ NĐ-CP | Nghị định | CNTT, điện tử | Quy định chi tiết điều kiện kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng |
| 898/ QĐ-TTg | Quyết định | CNTT, điện tử | Phê duyệt phương hướng, mục tiêu, nhiệm vụ bảo đảm an toàn thông tin mạng giai đoạn 2016 - 2020 |
| 86/ 2015/ QH13 | Luật | Viễn thông, CNTT, điện tử | Quy định về hoạt động an toàn thông tin mạng, quyền, trách nhiệm của cơ quan, tổ chức, cá nhân; mật mã dân sự; tiêu chuẩn, quy chuẩn kỹ thuật; kinh doanh trong lĩnh vực và phát triển nguồn nhân lực an toàn thông tin mạng; quản lý nhà nước. |
| 1883/ QĐ-BTTTT | Quyết định | Cơ cấu tổ chức | Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Trung tâm Tư vấn và hỗ trợ nghiệp vụ an toàn thông tin |
| 893/ QĐ-TTg | Quyết định | CNTT, điện tử | Phê duyệt Đề án Tuyên truyền, phổ biến, nâng cao nhận thức và trách nhiệm về an toàn thông tin đến năm 2020 |
| 1281/ QĐ-BTTTT | Quyết định | CNTT, điện tử, Cơ cấu tổ chức | Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Cục An toàn thông tin |
| 05/ 2014/ TT-BTTTT | Thông tư | Lĩnh vực khác | Thông tư Quy định Danh mục sản phẩm, hàng hóa có khả năng gây mất an toàn thuộc trách nhiệm quản lý của Bộ Thông tin và Truyền thông |
| 99/ QĐ-TTg | Quyết định | CNTT, điện tử | Phê duyệt Đề án "đào tạo và phát triển nguồn nhân lực an toàn, an ninh thông tin đến năm |

| | | | |
|---|---|---|---|
| | | | 2020" |
| 22/ 2013/ QĐ-UBND | Quyết định | CNTT, điện tử | Ban hành Quy chế đảm bảo an toàn, an ninh thông tin trên môi trường mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Bến Tre |
| 23/ 2011/ TT-BTTTT | Thông tư | Viễn thông, CNTT, điện tử, Lĩnh vực khác | Quy định về việc quản lý, vận hành, sử dụng và bảo đảm an toàn thông tin trên Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước |
| 20/ 2011/ TT-BTTTT | Thông tư | Viễn thông, CNTT, điện tử | Quy định danh mục sản phẩm, hàng hóa có khả năng gây mất an toàn thuộc trách nhiệm quản lý của Bộ Thông tin và Truyền thông |
| 897/ CT-TTg | Chỉ thị | CNTT, điện tử, Lĩnh vực khác | V/v tăng cường triển khai các hoạt động đảm bảo an toàn thông tin số |
| 25/ 2010/ TT-BTTTT | Thông tư | CNTT, điện tử | Quy định việc thu thập, sử dụng, chia sẻ, đảm bảo an toàn và bảo vệ thông tin cá nhân trên trang thông tin điện tử hoặc cổng thông tin điện tử của cơ quan nhà nước |
| 04/ CT-BTTTT | Chỉ thị | Viễn thông | Về tăng cường công tác quản lý, kiểm tra việc sử dụng điện thoại không dây để đảm bảo an toàn cho các hệ thống thông tin vô tuyến điện. |
| 06/ 2008/ TTLT-BTTTT-BCA | Thông tư | Viễn thông, Lĩnh vực khác | Về bảo đảm an toàn cơ sở hạ tầng và an ninh thông tin trong hoạt động bưu chính, viễn thông và công nghệ thông tin |
| 30/ 2007/ CT-TTg | Chỉ thị | Viễn thông | Về việc tăng cường bảo vệ các tuyến cáp viễn thông ngầm trên biển và bảo đảm an toàn viễn thông quốc tế |
| 06/ 2004/ CT-BBCVT | Chỉ thị | Viễn thông | Tăng cường đảm bảo an toàn, an ninh thông tin Bưu chính, Viễn thông và Internet trong tình hình mới |
| 71/ 2004/ QĐ-BCA (A11) | Quyết định | Lĩnh vực khác | Quyết định 71/2004/QĐ-BCA(A11) của Bộ Công an về việc ban hành Quy định về đảm bảo an toàn, an ninh trong hoạt động quản lý, cung cấp, sử dụng dịch vụ Internet tại Việt Nam |

### 7.2.2 *Các hành vi bị ngăn chặn và điều chỉnh*

Phần dưới đây trình bày về các hành vi về lĩnh vực an toàn thông tin được điều chỉnh bởi các văn bản pháp luật Việt Nam.

a. *Luật giao dịch điện tử 51/2005/QH11*

Luật Giao dịch điện tử số 51/2005/QH11 được QH thông qua 29/11/2005 xác định các hành vi không được phép trong các giao dịch điện tử trong Điều 9 cụ thể:

Điều 9. Các hành vi bị nghiêm cấm trong giao dịch điện tử

1. Cản trở việc lựa chọn sử dụng giao dịch điện tử.
2. Cản trở hoặc ngăn chặn trái phép quá trình truyền, gửi, nhận thông điệp dữ liệu.
3. Thay đổi, xoá, huỷ, giả mạo, sao chép, tiết lộ, hiển thị, di chuyển trái phép một phần hoặc toàn bộ thông điệp dữ liệu.
4. Tạo ra hoặc phát tán chương trình phần mềm làm rối loạn, thay đổi, phá hoại hệ thống điều hành hoặc có hành vi khác nhằm phá hoại hạ tầng công nghệ về giao dịch điện tử.
5. Tạo ra thông điệp dữ liệu nhằm thực hiện hành vi trái pháp luật.
6. Gian lận, mạo nhận, chiếm đoạt hoặc sử dụng trái phép chữ ký điện tử của người khác.

b. *Luật CNTT 2006*

Luật Công nghệ thông tin là công cụ để tạo hành lang pháp lý quan trọng cho việc thực hiện mục tiêu hình thành, phát triển xã hội thông tin. Luật Công nghệ thông tin là cơ sở pháp lý quan trọng để xác định rõ trách nhiệm quản lý nhà nước về Công nghệ thông tin của Chính phủ và các cơ quan quản lý nhà nước.

Chương I trình bày phạm vi điều chỉnh, đối tượng áp dụng, quyền và trách nhiệm của tổ chức, cá nhân tham gia hoạt động ứng dụng và phát triển công nghệ thông tin, thanh tra công nghệ thông tin, hiệp hội công nghệ thông tin và các hành vi bị nghiêm cấm.

Chương IV trình bày các biện pháp bảo đảm ứng dụng và phát triển công nghệ thông tin trong đó:

- Mục 1. Quy định về phát triển và đảm bảo cơ sở hạ tầng thông tin cho ứng dụng cũng như phát triển công nghệ thông tin cho cơ quan nhà nước
- Mục 2. Quy định cụ thể về Đầu tư của tổ chức, cá nhân và cơ quan nhà nước cho công nghệ thông tin;
- Mục 3. Quy định nguyên tắc, nội dung hợp tác quốc tế về công nghệ thông tin nhằm tạo điều kiện cho các thành phần kinh tế mở rộng hợp tác với tổ chức và cá nhân nước ngoài
- Mục 4. Mục này quy định về trách nhiệm của nhà nước, xã hội trong việc
  - Bảo vệ quyền và lợi ích hợp pháp của người sử dụng;
  - Bảo vệ tên miền quốc gia;
  - Bảo vệ quyền sở hữu trí tuệ trong lĩnh vực công nghệ thông tin;
  - Chống thư rác, vi rút máy tính và phần mềm gây hại;

- Bảo vệ trẻ em tránh những thông tin tiêu cực;
- Bảo đảm an toàn, bí mật thông tin;
- Hỗ trợ người tàn tật trong ứng dụng và phát triển công nghệ thông tin.

c. *Luật hình sự*

Luật hình sự sửa đổi bổ sung 2009/Chương XIX cho bộ luật 1999 (có hiệu lực từ 1/1/2010) xác định các hành vi tội phạm mạng trong các điều khoản :

- Điều 224. Tội phát tán vi rút, chương trình tin học có tính năng gây hại cho hoạt động của mạng máy tính, mạng viễn thông, mạng Internet, thiết bị số
- Điều 225. Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, mạng Internet, thiết bị số
- Điều 226. Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông, mạng Internet:
  - Điều 226a. Tội truy cập bất hợp pháp vào mạng máy tính, mạng viễn thông, mạng Internet hoặc thiết bị số của người khác
  - Điều 226b. Tội sử dụng mạng máy tính, mạng viễn thông, mạng Internet hoặc thiết bị số thực hiện hành vi chiếm đoạt tài sản

d. *Luật an toàn thông tin mạng 2015*

Ngày 19/11/2015, kỳ họp thứ mười Quốc hội Khóa XIII đã thông qua dự án Luật an toàn thông tin mạng. Luật này quy định về hoạt động an toàn thông tin mạng bao gồm các lĩnh vực:

- Bảo đảm an toàn thông tin trên mạng;
- Mật mã dân sự;
- Tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin mạng;
- Kinh doanh trong lĩnh vực an toàn thông tin mạng;
- Phát triển nguồn nhân lực an toàn thông tin mạng;
- Quản lý nhà nước về an toàn thông tin mạng;
- Quyền và nghĩa vụ của tổ chức, cá nhân tham gia hoạt động an toàn thông tin mạng.

Các nhóm hành vi bị nghiêm cấm theo luật này:

- Ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật.
- Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng truy nhập hệ thống thông tin của người sử dụng.
- Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin mạng của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin.

- Phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.
- Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân.
- Xâm nhập trái pháp luật bí mật mật mã và thông tin đã mã hóa hợp pháp của cơ quan, tổ chức, cá nhân; tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự; sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc.

e. *Luật an ninh mạng 2018*

Bộ luật này được xây dựng nhằm quy định về hoạt động bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội trên không gian mạng; trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan.

Các hành vi bị nghiêm cấm và điều chỉnh bao gồm:

- Điều 8 của Luật này quy định các hành vi bị nghiêm cấm trên môi trường mạng tiêu biểu như việc sử dụng không gian mạng để lan truyền thông tin trái phép hoặc sai sự thật; thực hiện các hành vi tấn công lên hệ thống thông tin quan trọng quốc gia; sử dụng hay sản xuất các thiết bị phần cứng và mềm gây cản trở hoạt động bình thường của các hệ thống mạng.
  Các hành vi chống lại lực lượng bảo vệ an ninh mạng và xâm phạm đến chủ quyền lợi ích và an ninh quốc gia cũng bị nghiêm cấm.
- Khoản 3 Điều 26 của Luật yêu cầu doanh nghiệp trong nước và nước ngoài cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu về thông tin cá nhân phải lưu trữ dữ liệu này tại Việt Nam trong thời gian theo quy định của Chính phủ.
  Riêng doanh nghiệp nước ngoài phải đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam.
- Doanh nghiệp phải cung cấp thông tin người dùng để phục vụ điều tra và phải có trách nhiệm xác thực thông tin khi người dùng đăng ký tài khoản số; bảo mật thông tin, tài khoản của người dùng. Đặc biệt, phải cung cấp thông tin người dùng cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi có yêu cầu bằng văn bản để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng.
  Khi người dùng chia sẻ những thông tin bị nghiêm cấm, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam phải ngăn chặn việc chia sẻ thông tin, xóa bỏ thông tin vi phạm chậm nhất là 24 giờ, kể từ thời điểm có yêu cầu của lực

lượng bảo vệ an ninh mạng thuộc Bộ Công an hoặc cơ quan của Bộ Thông tin và Truyền thông.

### 7.2.3 *Các điều kiện với các hoạt động trong môi trường mạng*

Phần dưới đây trình bày các điều kiện được ràng buộc bởi các văn bản pháp luật với các cá nhân và tổ chức tham gia hoạt động trong lĩnh vực CNTT, mạng và an toàn thông tin.

a. *Nghị định 160/2004/NĐ-CP*

Nghị định quy định chi tiết thi hành một số điều của Pháp lệnh Bưu chính, Viễn thông về viễn thông cụ thể:

- Điều 3 về bảo đảm an toàn mạng viễn thông và an ninh thông tin của Nghị định cho thấy mọi tổ chức, cá nhân phải bảo đảm an toàn mạng viễn thông và an ninh thông tin, thực hiện các yêu cầu về bảo đảm an ninh thông tin của các cơ quan Nhà nước có thẩm quyền; Bộ Bưu chính, Viễn thông phối hợp với một số Bộ, ngành liên quan hướng dẫn việc bảo đảm an toàn, an ninh thông tin trong hoạt động viễn thông.
- Điều 4 về bảo đảm bí mật thông tin cho thấy mọi tổ chức, cá nhân phải chịu trách nhiệm về nội dung thông tin mà mình đưa vào, lưu trữ và truyền đi trên mạng viễn thông; Nghiêm cấm việc trộm cắp thông tin, sử dụng trái phép mật khẩu, mật mã và thông tin riêng của các tổ chức cá nhân.

b. *Luật giao dịch điện tử 51/2005/QH11*

Luật Giao dịch điện tử số 51/2005/QH11 được QH thông qua 29/11/2005 xác định điều kiện đảm bảo cho các giao dịch trong Điều 22 và 41 cụ thể:

Điều 22. Điều kiện để bảo đảm an toàn cho chữ ký điện tử. Chữ ký điện tử được xem là bảo đảm an toàn nếu được kiểm chứng bằng một quy trình kiểm tra an toàn do các bên giao dịch thỏa thuận và đáp ứng được các điều kiện sau đây:

- Dữ liệu tạo chữ ký điện tử chỉ gắn duy nhất với người ký trong bối cảnh dữ liệu đó được sử dụng;
- Dữ liệu tạo chữ ký điện tử chỉ thuộc sự kiểm soát của người ký tại thời điểm ký;
- Mọi thay đổi đối với chữ ký điện tử sau thời điểm ký đều có thể bị phát hiện;
- Mọi thay đổi đối với nội dung của thông điệp dữ liệu sau thời điểm ký đều có thể bị phát hiện.

Chữ ký điện tử đã được tổ chức cung cấp dịch vụ chứng thực chữ ký điện tử chứng thực được xem là bảo đảm các điều kiện an toàn quy định tại khoản 1 Điều này.

Điều 41. Bảo đảm an toàn, bảo mật và lưu trữ thông tin điện tử trong cơ quan nhà nước:

- Định kỳ kiểm tra và bảo đảm an toàn hệ thống thông tin điện tử của cơ quan mình trong quá trình giao dịch điện tử.
- Bảo đảm bí mật thông tin liên quan đến giao dịch điện tử, không được sử dụng thông tin vào mục đích khác trái với quy định về việc sử dụng thông tin đó, không tiết lộ thông tin cho bên thứ ba theo quy định của pháp luật.
- Bảo đảm tính toàn vẹn của thông điệp dữ liệu trong giao dịch điện tử do mình tiến hành; bảo đảm an toàn trong vận hành của hệ thống mạng máy tính của cơ quan mình.
- Thành lập cơ sở dữ liệu về các giao dịch tương ứng, bảo đảm an toàn thông tin và có biện pháp dự phòng nhằm phục hồi được thông tin trong trường hợp hệ thống thông tin điện tử bị lỗi.
- Bảo đảm an toàn, bảo mật và lưu trữ thông tin theo quy định của Luật này và các quy định khác của pháp luật có liên quan.

c. *Nghị định 97/2008/NĐ-CP*

Nghị định này quy định chi tiết về việc quản lý, sử dụng dịch vụ Internet và thông tin điện tử trên Internet tại Việt Nam.

- Điều 4 quy định về chính sách quản lý và phát triển Internet nêu rõ Internet Việt Nam là một bộ phận quan trọng thuộc cơ sở hạ tầng thông tin quốc gia, được bảo vệ theo pháp luật, không ai được xâm phạm. Bảo đảm an toàn, an ninh cho các hệ thống thiết bị và thông tin điện tử trên Internet là trách nhiệm của các cơ quan nhà nước, mọi tổ chức và cá nhân.
- Điều 7 quy định doanh nghiệp cung cấp dịch vụ Internet có trách nhiệm triển khai các trang thiết bị và phương án kỹ thuật, nghiệp vụ bảo đảm an toàn, an ninh thông tin theo hướng dẫn của cơ quan nhà nước có thẩm quyền;
- Điều 8 quy định các chủ mạng Internet dùng riêng có trách nhiệm thực hiện các quy định về cấp phép, kết nối, tiêu chuẩn, chất lượng, giá cước, an toàn, an ninh thông tin, tài nguyên Internet.
- Điều 9 quy định các đại lý Internet có trách nhiệm tuân thủ các quy định về đảm bảo an toàn, an ninh thông tin;
- Điều 10 quy định doanh nghiệp cung cấp hạ tầng mạng có trách nhiệm phối hợp với các cơ quan quản lý nhà nước, các doanh nghiệp cung cấp dịch vụ Internet trong công tác bảo đảm an toàn, an ninh thông tin và điều tra, ngăn chặn các hành vi vi phạm pháp luật trong hoạt động Internet.

d. *Nghị định 90/2008/ NĐ-CP*

Nghị định này ra đời ngày 13/08/2008 (hiện nay đã được điều chỉnh bổ sung với Nghị định 77/2012/NĐ-CP). Nghị định này quy định về chống thư rác; quyền và nghĩa vụ của cơ quan, tổ chức, cá nhân có liên quan. Phân loại Spam theo nghị định bao gồm:

- Email, tin nhắn di động với mục đích lừa đảo, quấy rối, phát tán vi rút máy tính và mã độc.
- Email và tin nhắn quảng cáo vi phạm quy tắc gửi tin nhắn và email quảng cáo.

e. *Luật an toàn thông tin mạng*

Bộ luật đề ra các yêu cầu về bảo vệ thông tin mạng trong đó tổ chức sở hữu thông tin phân loại thông tin để có biện pháp bảo vệ phù hợp:

- Phân loại thông tin theo thuộc tính bí mật để có biện pháp bảo vệ phù hợp
- Xây dựng quy định, thủ tục để xử lý thông tin đã phân loại và chưa phân loại,
- Xác định nội dung và phương pháp ghi truy nhập được phép vào thông tin đã được phân loại.

Thông tin thuộc phạm vi bí mật nhà nước được phân loại và bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước.

Đối với việc quản lý gửi thông tin, bộ luật yêu cầu:

- Không giả mạo nguồn gốc gửi thông tin;
- Thông tin thương mại cần được sự đồng ý hay yêu cầu của người nhận
- Doanh nghiệp cung cấp dịch vụ
  - Đảm bảo việc lưu trữ thông tin và bảo vệ thông tin cá nhân và tổ chức
  - Áp dụng biện pháp ngăn chặn khi có hành vi gửi thông tin vi phạm pháp luật
  - Có phương thức để người nhận từ chối nhận thông tin
- Doanh nghiệp cung cấp dịch vụ thư điện tử, truyền tin, lưu trữ thông tin phải có hệ thống lọc phần mềm độc hại trong quá trình gửi, nhận, lưu trữ thông tin trên hệ thống của mình
- Doanh nghiệp cung cấp dịch vụ Internet có biện pháp quản lý, phát hiện, ngăn chặn phát tán thông tin, phần mềm độc hại, thư rác và xử lý theo yêu cầu của cơ quan nhà nước có thẩm quyền.

Bộ luật đề ra các cấp độ với việc bảo vệ hệ thống thông tin gồm có

- Cấp độ 1: Khi bị phá hoại sẽ làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân nhưng không làm tổn hại tới lợi ích công cộng, trật tự an toàn xã hội, quốc phòng, an ninh quốc gia;
- Cấp độ 2: Khi bị phá hoại sẽ làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng nhưng không làm tổn hại tới trật tự an toàn xã hội, quốc phòng, an ninh quốc gia;
- Cấp độ 3: Khi bị phá hoại sẽ làm tổn hại nghiêm trọng tới sản xuất, trật tự xã hội và lợi ích công cộng hoặc tạo thành tổn hại tới quốc phòng, an ninh quốc gia;

- Cấp độ 4: Khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng và trật tự an toàn xã hội hoặc tạo thành tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia;
- Cấp độ 5: Khi bị phá hoại sẽ tạo thành tổn hại đặc biệt nghiêm trọng tới quốc phòng, an ninh quốc gia.

### 7.2.4 *Các trọng tâm quản lý nhà nước về an toàn thông tin*

Các hệ thống mạng và các ứng dụng sử dụng mạng ngày càng phát triển và phổ cập rộng rãi trong các hoạt động thường ngày của mỗi người. Bên cạnh sự nhanh chóng và thuận tiện do các hệ thống và ứng dụng mang lại, vấn đề về an toàn thông tin ngày càng trở nên quan trọng và phức tạp. Để ứng phó và đáp ứng tốt hơn các thay đổi và tiến bộ trong lĩnh vực này, nhà nước xác định các trọng tâm cho việc quản lý sự phát triển của các hệ thống mạng và ứng dụng như sau:

- Tiếp tục hoàn thiện cơ sở pháp lý. Ban hành các văn bản quy phạm pháp luật cần thiết nhằm trấn áp các hoạt động phá hoại thông tin
- Tăng cường phổ biến và khuyến nghị các doanh nghiệp, các cơ quan nhà nước, cộng đồng xã hội triển khai các hệ thống phòng thủ, bảo vệ phù hợp theo các tiêu chuẩn, hướng dẫn đã ban hành.
- Khuyến nghị các cơ quan tổ chức, các ISP triển khai rà soát thường xuyên hệ thống thông tin, vá các lỗ hổng an ninh, cài đặt lại cấu hình an toàn; tăng cường kiểm soát truy nhập hệ thống; đánh giá rủi ro.
- Nhà nước phối hợp với các doanh nghiệp cung cấp dịch vụ viễn thông tổ chức kênh tuyên truyền trực tiếp qua thư điện tử, tin nhắn tới người dân về các nguy cơ mất an toàn, an ninh thông tin
- Tăng cường tổ chức, phối hợp giữa các đơn vị tư vấn, chuyên gia an toàn, an ninh thông tin sẵn sàng ứng phó với những sự cố liên quan tới mất an toàn, an ninh thông tin
- Thành lập các trung tâm ứng cứu sự cố máy tính tại các địa phương, đây là các đơn vị đầu mối của các địa phương về việc đảm bảo an toàn, an ninh thông tin tại mỗi địa phương
- Khuyến nghị các cơ quan tổ chức xây dựng chính sách an toàn thông tin, các quy trình đảm bảo an toàn thông tin; nâng cao nhận thức về an toàn, an ninh thông tin cho lãnh đạo và cán bộ
- Phát triển nhân lực, mạng lưới chuyên gia có chứng chỉ cần thiết về an toàn thông tin
- Xây dựng hệ thống theo dõi, giám sát, cảnh báo sớm; Hệ thống ghi dấu vết, bằng chứng điện tử
- Tăng cường công tác thanh tra, kiểm tra; đảm bảo sự thực thi của pháp luật

## 7.3 Hệ thống pháp luật an toàn thông tin của các nước

### 7.3.1 *Luật và tổ chức quốc tế*

Hiệp định Ủy ban Châu Âu về tội phạm mạng (Council of Europe Convention on CyberCrime) được xây dựng vào 2001. Tổ chức này hướng tới việc giám sát các chức năng an toàn liên quan tới các hoạt động Internet đối với các luật về công nghệ. Đồng thời, tổ chức này cải thiện tính hiệu quả của việc điều tra quốc tế về các vi phạm.

Tổ chức thương mại quốc tế WTO (World Trade Organisation) đề xuất thỏa thuận về các khía cạnh thương mại của quyền sở hữu trí tuệ bao gồm cách thức:

- Các nguyên tắc căn bản của hệ thống thương mại và các thỏa thuận về sở hữu trí tuệ phải được áp dụng
- Bảo vệ quyền sở hữu trí tuệ
- Thực thi một cách thích đáng các quyền này tại quốc gia sở tại
- Dàn xếp các tranh chấp
- Thoả thuận chuyển đổi đặc biệt trong thời gian hệ thống được đưa ra.

Tổ chức thế giới về sở hữu trí tuệ (WIPO) đề xuất luật bản quyền số thiên niên kỷ (DMCA) với đóng góp của Mỹ bao gồm các điều khoản:

- Nghiêm cấm việc xâm phạm việc bảo vệ và các biện pháp được thực thi bởi người có bản quyền để kiểm soát việc truy nhập vào nội dung được bảo vệ.
- Nghiêm cấm việc sản xuất các thiết bị xâm phạm các cơ chế bảo vệ và các biện pháp truy nhập vào nội dung được bảo vệ
- Cấm việc buôn lậu các thiết bị xâm phạm việc bảo vệ các biện pháp kiểm soát việc truy nhập nội dung; Nghiêm cấm việc sửa đổi thông tin đính kèm hay nhúng vào các tư liệu bản quyền
- Loại bỏ các nhà cung cấp dịch vụ Internet khỏi các dạng nhất định giúp cho việc vi phạm bản quyền.

Ngoài các tổ chức quốc tế kể trên, các hợp tác và liên kết trong khu vực cũng có các nỗ lực đưa ra các thỏa thuận và ghi nhớ chung về an toàn thông tin gồm có:

- Nghị quyết Hội nghị cấp cao 10 của các nước APEC ở Lốt Ca-bốt, Mê-hi-cô năm 2002 thông qua tuyên bố chung về an toàn thông tin, trong đó có nêu các vấn đề về xây dựng luật và các văn bản pháp luật, công ước quốc tế về an toàn thông tin.
- Nghị quyết Hội nghị Cấp cao ASEM 5 (2004 tại Hà Nội) thông qua 9 sáng kiến hợp tác, trong đó có sáng kiến 6 là về tăng cường an toàn mạng trong khu vực ASEM.
- Các cam kết trong Liên minh Viễn thông Quốc tế (ITU), Tổ chức Viễn thông Châu Á Thái Bình Dương (APECTel).

- Nghị quyết các Hội nghị quan chức cấp cao viễn thông (TELSOM) và Hội nghị Bộ trưởng Viễn thông (TELMIN) tổ chức hàng năm đều có các khuyến nghị cho các nước về lĩnh vực an toàn thông tin.

### 7.3.2 *Luật pháp an toàn thông tin của Mỹ*

Phần dưới đây giới thiệu các đạo luật quan trọng của Mỹ về lĩnh vực an toàn thông tin.

a. *Luật gian lận và lạm dụng máy tính năm 1986*

Đạo luật CFA (Computer Fraud and Abuse Act ) này là nền tảng của nhiều luật liên bang liên quan đến máy tính. Điều 18 Hiến pháp Hoa kỳ, mục 1030, đã đưa vào từ năm 1984, từ đó được bổ sung một số lần:

- Sửa đổi 10/1996: Đạo luật bảo vệ Hệ thống thông tin Quốc gia, tăng mức hình phạt, bổ sung loại hình tội phạm.
- Sửa đổi năm 2001: theo Đạo luật Yêu nước (Patriot Act): Tăng cường và hợp nhất luật Mỹ thông qua việc cung cấp các thiết chế thích hợp để bổ sung cho Đạo luật ngăn chặn và chống khủng bố 2001. Bổ sung công nghệ cao, bổ sung phạm vi thực thi pháp luật.

Đạo luật này nghiêm cấm xâm nhập, làm hỏng và truy nhập trái phép tới các máy tính được bảo vệ. Khái niệm "máy tính được bảo vệ" được phân loại như sau:

- Loại A: cơ quan tài chính hoặc Chính phủ Mỹ
- Loại B: thương mại, thông tin liên lạc, dân dụng, ngoại thương, kể cả máy tính để ở ngoài nước Mỹ

Đạo luật CFA cấm các hành vi:

- Truy nhập trái phép tới máy tính đang chứa các dữ liệu về quốc phòng, quan hệ quốc tế hoặc các dữ liệu hạn chế của Chính phủ liên bang.
- Truy nhập trái phép tới máy tính chứa các thông tin nhất định về tài chính và ngân hàng.
- Truy nhập trái phép, sử dụng, xuyên tạc (thay đổi), thay đổi cấu trúc, hoặc làm lộ về máy tính hoặc thông tin trong máy tính làm việc nhân danh và vì lợi ích của Chính phủ Mỹ.
- Sự truy nhập không có cho phép một "máy tính được bảo hộ", mà toà án hiện đang chỉ định đối với bất kỳ máy tính nào đó được kết nối với Internet.
- Các gian lận máy tính.
- Lan truyền các mã gây hại các hệ thống máy tính hoặc các mạng.
- Buôn bán các mật khẩu máy tính

b. *Đạo luật bảo vệ các liên lạc điện tử (Electronic Communications Act):*

Đạo luật này nghiêm cấm các can thiệp bất hợp pháp, tiết lộ các liên lạc điện tử được truyền tải hoặc lưu trong mạng truyền thông bao gồm:

- Chống nghe trộm các liên lạc truyền thông.
- Bảo vệ liên lạc điện tử bất kỳ sự truyền tải các ký hiệu, tín hiệu, chữ viết, hình ảnh, âm thanh, dữ liệu, hoặc tri thức được truyền toàn bộ hoặc từng phần bằng hệ thống vô tuyến, hữu tuyến, điện tử, điện quang hay quang học, có tác động tới thương mại toàn liên bang hoặc ngoại thương".
- Bảo vệ chống can thiệp trong khi truyền tải.
- Các hình phạt và quyền bảo hộ chống các hành vi làm tổn hại, bồi thường và chi phí liên quan.
- Thủ tục truy nhập hợp pháp của các cơ quan thực thi pháp luật. Quyền truy nhập theo lệnh của Toà án vào các liên lạc hoặc các bản ghi. Yêu cầu các ISP cài đặt thiết bị cần thiết cho phép các cuộc nghe lén theo lệnh của Toà án. Cho phép các ISP đọc nội dung các liên lạc nhằm duy trì dịch vụ hoặc tự bảo vệ.Ví dụ, nhà cung cấp dịch vụ có thể ghi dữ liệu để phát hiện và loại trừ virus.

c. *Đạo luật An toàn máy tính (1987 – Computer Security Act): đưa ra các quy định tối thiểu để bảo vệ hệ thống máy tính bằng các biện pháp an ninh:*
   - Phát triển các tiêu chuẩn, hướng dẫn, phương pháp và kỹ thuật liên quan cho các hệ thống máy tính.
   - Phát triển các tiêu chuẩn, hướng dẫn về quản lý, kỹ thuật cho việc bảo mật hiệu quả và bảo mật thông tin nhạy cảm trong các hệ thống máy tính liên bang.
   - Xây dựng hướng dẫn khai thác, vận hành, nâng cao nhận thức.
   - Xây dựng các thủ tục kiểm chứng, đánh giá bảo mật.

   Các hệ thống an ninh quốc gia được xác định :
   - Bất kỳ hệ thống thông tin nào (kể cả hệ thống viễn thông) được sử dụng hoặc vận hành bởi cơ quan Nhà nước hoặc tổ chức do cơ quan Nhà nước ủy quyền, mà trong đó chức năng, sự hoạt động hay sử dụng hệ thống kéo theo có chứa đựng một trong các hoạt động tình báo, hoạt động mật mà liên quan đến an ninh quốc gia;
   - Việc quản lý và chỉ huy lực lượng vũ trang, các thiết bị hay thành phần tích hợp của hệ thống vũ khí, các hệ thống hành chính và kinh doanh đáp ứng trực tiếp nhiệm vụ quân sự hay tình báo.
   - Các hệ thống thông tin được bảo vệ liên tục theo quy định của Pháp luật hoặc được Chính Phủ xếp loại thiết yếu đối với cơ quan hay đối ngoại.

   Các hệ thống hành chính và kinh doanh thông thường (kể cả hệ thống tài chính, hậu cần, trả lương hay quản lý nhân sự) đều không thuộc các hệ thống an ninh Quốc gia.

   Các nội dung chính của đạo luật quy định
   - Quyền và chức năng người đứng đầu các cơ quan Nhà nước
   - Trách nhiệm cơ quan Chính Phủ
   - Đánh giá hàng năm

- Trung Tâm ứng cứu sự cố an toàn thông tin
- Hệ thống an ninh quốc gia
- Ủy quyền: Thực hiện các quy định cho mỗi năm

d. *Luật quản lý an toàn thông tin Liên Bang – FISMA 2002 (Federal Information Security Management Act):*

Đạo luật này nhằm bảo vệ thông tin và các hệ thống thông tin trong môi trường thông tin khỏi các hành vi truy cập, sử dụng, khai thác, làm hỏng, phá hủy hay sửa đổi một cách trái phép nhằm đảm bảo:

- Tính toàn vẹn, có nghĩa là bảo vệ chống việc sửa đổi hay phá hỏng thông tin bao gồm khả năng chống chối bỏ và xác thực của thông tin.
- Tính bí mật, có nghĩa là giữ quyền truy cập và khai thác thông tin, bao gồm việc bảo vệ thông tin cá nhân và thông tin đúng đối tượng.
- Tính sẵn dùng, có nghĩa là đảm bảo khả năng truy cập và sử dụng thông tin kịp thời và tin cậy

e. *Luật an toàn không gian mạng (Cybersecuirty Act)*

Ngày 18 tháng 12 năm 2015, Tổng thống Obama đã ký thành luật Đạo luật an ninh mạng năm 2015. Đạo luật thiết lập cơ chế chia sẻ thông tin an ninh mạng giữa các tổ chức chính phủ và khu vực tư nhân. Đạo luật này cũng cung cấp các yêu cầu an toàn về trách nhiệm của các thực thể tư nhân chia sẻ thông tin an ninh mạng theo các thủ tục nhất định và cho phép các thực thể khác nhau, bao gồm cả bên ngoài chính phủ liên bang giám sát các hệ thống thông tin nhất định và vận hành các biện pháp phòng thủ cho mục đích an ninh mạng.

Đạo luật cũng bao gồm các điều khoản được thiết kế để tăng cường bảo vệ an ninh mạng tại các cơ quan liên bang, đánh giá lực lượng an ninh không gian mạng của chính phủ liên bang và thực hiện một loạt các biện pháp nhằm cải thiện và chuẩn bị an ninh mạng của các hệ thống thông tin và mạng quan trọng.

Bộ luật gồm 4 nội dung quan trọng:

- Chương I thiết lập một cơ chế tập trung để chia sẻ thông tin an ninh mạng. Nội dung này là quan tâm lớn nhất đối với hầu hết các tổ chức khu vực tư nhân.
- Chương II hướng dẫn Bộ an ninh nội địa thực hiện các biện pháp được thiết kế để tăng cường an ninh mạng trong chính phủ liên bang và tại các cơ quan liên bang, cũng như tạo thuận lợi cho việc thực hiện nội dung Chương I.
- Chương III tập trung đánh giá an ninh không gian mạng của lực lượng liên bang.
- Chương IV quy định các biện pháp khác nhằm xác định và giải quyết các mối đe dọa đối với các hệ thống và mạng thông tin quan trọng.

### 7.3.3 *Luật pháp an toàn thông tin của Châu Âu*

Những tiêu chuẩn về an ninh mạng đã nhận được sự quan tâm đặc biệt trong kỷ nguyên bùng nổ ứng dụng trên Internet. Cộng đồng EU mong muốn đưa ra các quy định phù hợp cho các doanh nghiệp hoạt động đặc biệt trong Liên minh châu Âu. Ba bộ phận tạo nên luật an ninh mạng trong EU bao gồm ENISA, chỉ thị về an ninh mạng và an ninh thông tin (NIS) và tiêu chuẩn bảo vệ dữ liệu chung của EU (EU GDPR).

a. *ENISA*

Đây là cơ quan về an ninh mạng và an ninh thông tin của Liên minh châu Âu EU ban đầu được thành lập theo các Quy định (EC) số 460/2004 của Nghị viện Châu Âu và của Hội đồng Liên minh châu Âu vào năm 2004 với mục đích nâng cao an ninh mạng và an ninh thông tin, chỉ thị về an ninh mạng và an ninh thông tin (NIS) và nhận thức cho tất cả các hoạt động liên mạng bên trong EU. ENISA hiện thời hoạt động theo Quy định (EU) số 526/2013 để thay thế các quy định ban đầu vào năm 2013. ENISA tích cực hợp tác với tất cả các nước thành viên của Liên minh châu Âu. Trọng tâm của các hoạt động của họ tập trung vào ba yếu tố chính sau:

- Khuyến nghị các nước thành viên về quá trình hành động đối với vi phạm an ninh mạng
- Xây dựng chính sách và hỗ trợ vấn đề thực hiện cho tất cả các thành viên EU
- Hỗ trợ trực tiếp - ENISA trực tiếp làm việc với các đội nhóm hoạt động bên trong EU

ENISA đã phát hành các tài liệu khác nhau bao quát tất cả các vấn đề quan trọng liên quan đến an ninh mạng. Sáng kiến trước đây và hiện tại của ENISA bao gồm: Chiến lược đám mây EU, các tiêu chuẩn mở trong công nghệ truyền thông thông tin, Chiến lược an ninh mạng của EU và nhóm điều phối an ninh mạng. ENISA cũng hợp tác với các tổ chức tiêu chuẩn quốc tế hiện thời như ISO và ITU.

b. *Chỉ thị về An ninh mạng và An ninh thông tin (NIS)*

Vào ngày 6 tháng 7 năm 2016, Nghị viện châu Âu đưa Chỉ thị về an ninh của mạng và hệ thống thông tin (chỉ thị NIS) thành chính sách. Chỉ thị này có hiệu lực vào tháng 8 năm 2016 và tất cả các quốc gia thành viên của Liên minh châu Âu có 21 tháng để tích hợp các luật lệ của chỉ thị này vào luật quốc gia riêng của họ. Mục đích của Chỉ thị NIS này là tạo ra một mức độ an ninh mạng tổng thể cao hơn trong EU. Chỉ thị này có ảnh hưởng đáng kể đến các nhà cung cấp dịch vụ kỹ thuật số, các công nghệ xử lý tín hiệu số DSP và các nhà khai thác dịch vụ thiết yếu OES.

Các nhà khai thác dịch vụ thiết yếu bao gồm bất kỳ tổ chức nào mà hoạt động của họ sẽ bị ảnh hưởng nghiêm trọng trong trường hợp có lỗ hổng an ninh mạng miễn là họ tham gia vào các hoạt động xã hội hoặc kinh tế quan trọng. Cả DSP và OES hiện đang chịu trách nhiệm trong việc báo cáo các sự cố an ninh cho các đội phản ứng nhanh với sự cố an ninh máy tính CSIRT. Trong khi DSP không phải chịu những quy định ngặt nghèo

như các nhà khai thác dịch vụ thiết yếu, DSP không được thành lập trong EU nhưng hoạt động trong EU vẫn phải đối mặt với các quy định này. Ngay cả khi DSP và OES thuê ngoài việc duy trì các hệ thống thông tin của họ cho bên thứ ba, Chỉ thị NIS vẫn bắt họ phải chịu trách nhiệm cho bất kỳ sự cố an ninh nào.

Các quốc gia thành viên của EU được yêu cầu phải đưa ra chiến lược hoạt động với chỉ thị NIS bao gồm các đội CSIRT nói trên bên cạnh các cơ quan có thẩm quyền quốc gia (NCA) và các cơ quan điều phối (SPOC). Những nguồn lực này được trao trách nhiệm xử lý vi phạm an ninh mạng để giảm thiểu tác động của nó. Bên cạnh đó, tất cả các quốc gia thành viên của EU được khuyến khích chia sẻ thông tin an ninh mạng.

Những yêu cầu bảo mật của chỉ thị NIS bao gồm các biện pháp kỹ thuật quản lý rủi ro của hành vi vi phạm an ninh mạng bằng cách phòng ngừa. Bên cạnh đó, cả DSP và OES phải cung cấp thông tin cho phép đánh giá chuyên sâu hệ thống thông tin và chính sách bảo mật của họ. Như đã đề cập ở trên, tất cả các sự cố quan trọng phải được thông báo cho các đội CSIRT. Mức độ nghiêm trọng của sự cố an ninh mạng được xác định bởi số lượng người sử dụng sẽ bị ảnh hưởng bởi cuộc tấn công mạng cũng như khoảng thời gian xảy ra các sự cố và phạm vi địa lý của vụ việc.

c. *Tiêu chuẩn bảo vệ dữ liệu chung của EU (EU GDPR)*

Quy định chung về bảo vệ dữ liệu của EU, GDPR, ra đời vào ngày 14 tháng 4 năm 2016, tuy nhiên ngày thực thi là 25 tháng 5 năm 2018. Các quy định chung này nhằm mang lại một tiêu chuẩn thống nhất để bảo vệ dữ liệu giữa tất cả các nước thành viên trong EU. Sự thay đổi mà các quy định này sẽ mang lại bao gồm việc xác định lại biên giới địa lý. Quy định không chỉ áp dụng cho các tổ chức hoạt động trong EU mà còn áp dụng cho các tổ chức xử lý dữ liệu của bất kỳ cư dân nào của EU. Bất kể nơi nào dữ liệu được xử lý, nếu dữ liệu của một công dân EU đang được xử lý, các tổ chức hiện tại phải tuân theo quy định này. Tiền phạt cũng trở nên nặng hơn và có thể lên tới 20 triệu euro hay 4% doanh thu hàng năm. Ngoài ra, tương tự như những quy định trước đây, tất cả các hành vi vi phạm dữ liệu ảnh hưởng tới các quyền và sự tự do của những cá nhân cư trú tại EU phải được công bố trong vòng 72 giờ. Ban bảo vệ dữ liệu của EU (EDP) phải chịu trách nhiệm về tất cả các giám sát theo quy định của GDPR.

Sự đồng thuận đóng một vai trò quan trọng trong các quy định của GDPR. Các công ty nắm giữ dữ liệu liên quan đến công dân EU hiện thời cũng phải cung cấp cho các công dân quyền được từ chối chia sẻ dữ liệu dễ dàng như việc người dân đồng ý chia sẻ chúng. Ngoài ra, người dân cũng có thể hạn chế việc xử lý các dữ liệu được lưu trữ về họ; họ có thể chọn lựa để cho phép các công ty lưu trữ dữ liệu của họ nhưng không xử lý nó do đó điều này tạo ra một sự khác biệt rõ ràng.

Khác với các quy định trước đây, GDPR cũng hạn chế việc chuyển giao dữ liệu của một công dân ra bên ngoài EU hoặc cho một bên thứ ba mà không có sự đồng ý trước của công dân đó. Quy định dự thảo ePrivacy dự kiến sẽ được áp dụng từ ngày 25 tháng 5 năm 2018.

### 7.3.4 *Luật pháp an toàn thông tin của các nước trong khu vực*

Môi trường pháp lý an ninh không gian mạng khu vực tập trung nhiều vào luật bảo vệ dữ liệu. Tuy nhiên, quy định an ninh mạng rõ ràng không chỉ về bảo vệ dữ liệu. Hơn thế, quy định an ninh mạng dựa trên những mối quan ngại lớn hơn về các vấn đề như an ninh quốc gia và thực thi pháp luật, tính toàn vẹn của cơ sở hạ tầng, mạng và hệ thống quan trọng, bảo vệ quyền sở hữu trí tuệ và thông tin bí mật, ngoài các vấn đề chính sách khác.

Trong hầu hết các khu vực pháp lý được phát triển trong khu vực, những mối quan tâm rộng hơn này được giải quyết với các mức độ khác nhau trên cơ sở từng phần trong các lĩnh vực như luật hình sự, luật chống khủng bố, luật viễn thông, luật sở hữu trí tuệ và quản lý rủi ro công nghệ các yêu cầu áp dụng cho các ngành được quy định.

Quy định an ninh không gian mạng, như là một lĩnh vực riêng biệt, không chỉ đơn giản là việc chọn và gộp các luật đa dạng này lại với nhau. Quy định này tìm cách thiết lập các tiêu chuẩn trong các lĩnh vực như nhận dạng mối đe dọa, đánh giá rủi ro và các biện pháp giảm thiểu, phản ứng sự cố và tạo điều kiện chia sẻ thông tin. Nó tìm cách tạo ra cơ sở cho việc quản lý chủ động và thích nghi các rủi ro trên mạng.

a. *Khung bảo mật APEC*

Khu vực châu Á có một số quốc gia đầu tiên hướng tới các quy định bảo vệ dữ liệu dựa trên nguyên tắc toàn diện, đáng chú ý nhất là Nhật Bản, Hồng Kông và Ma Cao, đã thông qua luật năm 1988, 1995 và 2005. Thỏa thuận năm 2005 của Hiệp định Kinh tế Châu Á-Thái Bình Dương (APEC) về Khung Quyền riêng tư tạo ra động lực chính thức cho các nền kinh tế thành viên khác để thông qua luật bảo vệ dữ liệu toàn diện. Trong khuôn khổ Khung Quyền riêng tư của APEC, các quốc gia Malaysia, Philippines, Singapore, Hàn Quốc và Đài Loan đều tham gia vào nhóm các quốc gia có luật bảo vệ dữ liệu toàn diện. Trung Quốc đã chuyển sang bảo vệ dữ liệu theo một cách cứng rắn hơn nhiều. Indonesia đã đưa ra một số quy định về dữ liệu, đáng chú ý nhất là luật bản địa hóa dữ liệu có hiệu lực vào năm 2017.

Khung quyền riêng tư của APEC quy định một bộ nguyên tắc thu thập, xử lý và chuyển giao dữ liệu cá nhân tương tự trong cách tiếp cận nguyên tắc của tổ chức hợp tác và phát triển kinh tế về bảo vệ quyền riêng tư và luồng dữ liệu cá nhân, các nguyên tắc tuân thủ luật bảo vệ dữ liệu quốc gia của Châu Âu và Quy định bảo vệ dữ liệu chung mới. Yêu cầu cốt lõi là dữ liệu cá nhân được thu thập một cách công bằng với sự đồng ý tự nguyện, thông báo của đối tượng dữ liệu. Một khi đã thu thập dữ liệu sẽ được xử lý an toàn theo mục đích mà nó đã được thu thập.

Khung quyền riêng tư của APEC không quy định nhiệm vụ thông báo cho các nhà quản lý hoặc các đối tượng dữ liệu bị ảnh hưởng vi phạm bảo mật dữ liệu. Nhưng một số nền kinh tế thành viên APEC đã vượt ra ngoài các yêu cầu chính thức của Khung Quyền riêng tư và ban hành các yêu cầu vi phạm dữ liệu bắt buộc. Ấn Độ, Philippines, Hàn

Quốc và Đài Loan đều đã đi theo hướng này. Các nghĩa vụ thông báo vi phạm cụ thể theo từng ngành có thể thấy ở Nhật Bản và Trung Quốc. Các nghĩa vụ thông báo vi phạm dữ liệu tự nguyện (nhưng được khuyến khích) áp dụng ở Hồng Kông và Singapore. Xu hướng rõ ràng hướng tới các yêu cầu thông báo ràng buộc, lưu ý rằng Quy định bảo vệ dữ liệu chung của châu Âu đã thực hiện một bước đối với thông báo bắt buộc 72 giờ về vi phạm dữ liệu và hầu hết các tiểu bang của Hoa Kỳ có luật thông báo vi phạm.

b. *Sáng kiến bảo vệ mạng của Hồng Kông*

Vào năm 2016 tại Hồng Kông các ngân hàng Hồng Kông công bố Sáng kiến bảo vệ an toàn mạng CFI (Cybersecurity Fortification Initiative) với ba trụ cột chính.

- Khung đánh giá khả năng phục hồi của mạng dự kiến sẽ là một công cụ tự đánh giá cho các tổ chức để đánh giá tính dễ bị tổn thương đối với các rủi ro trên mạng. Mục tiêu là hỗ trợ và tinh chỉnh các đánh giá của các tổ chức về sự sẵn sàng phát hiện và ứng phó với các mối đe dọa trên mạng. Cốt lõi của sáng kiến này là quá trình tự đánh giá và đánh giá sẽ được bổ sung bằng "thử nghiệm mô phỏng tấn công mạng" với các kịch bản thử nghiệm mô phỏng dựa trên tri thức về đe dọa mạng thời gian thực.
- Chương trình phát triển chuyên nghiệp nhằm tăng số lượng và trình độ chuyên môn của các chuyên gia bảo mật mạng tại Hồng Kông. Hồng Kông đề xuất hợp tác với Viện Nghiên cứu Khoa học và Công nghệ Ứng dụng Hồng Kông và Viện Ngân hàng Hồng Kông để phát triển chương trình.
- Nền tảng chia sẻ thông tin mạng phù hợp với các sáng kiến an ninh mạng ở Hoa Kỳ, EU và các nơi khác. Chương trình an ninh mạng của Hồng Kông tìm cách cải thiện chia sẻ thông tin trong ngành về các mối đe dọa trên mạng như một phương tiện xác định tốt hơn và chứa các mối đe dọa mới xuất hiện. Nền tảng dự định phát triển cùng với Hiệp hội các ngân hàng Hồng Kông sẽ hỗ trợ thu thập, phân tích và chia sẻ các báo cáo đe dọa mạng chi tiết.

c. *"An ninh và có thể kiểm soát " của Trung Quốc*

Cách tiếp cận của Trung Quốc đối với quy định an ninh mạng đã thu hút sự quan tâm của quốc tế trong những năm qua. Việc thông qua Luật an ninh quốc gia vào mùa hè năm 2015 cùng với việc công bố dự thảo đầu tiên của Luật an ninh mạng quốc gia. Với việc thông qua Luật chống khủng bố tiếp theo vào tháng 1 năm 2016, bản dự thảo thứ hai của Luật an ninh mạng vào năm 2016 cho thấy xu hướng rõ ràng đối với khái niệm Công nghệ "an toàn và có thể kiểm soát" (*secure and controllable*) hướng tới việc tiếp cận và phê duyệt công nghệ của nhà nước thông qua chứng nhận thị trường (liên quan đến việc tiết lộ mã nguồn), các biện pháp địa phương hóa dữ liệu và hạn ngạch cụ thể cho việc sử dụng các công nghệ "an toàn và có thể kiểm soát".

Hướng quy định an ninh mạng tại Trung Quốc khá khác biệt và đặt ra những thách thức đặc biệt cho các doanh nghiệp đa quốc gia, mở rộng các cuộc điều tra xung quanh

công nghệ và chiến lược lưu trữ dữ liệu, bảo mật thông tin liên lạc và các vấn đề luật địa phương như nguy cơ sở hữu những bí mật nhà nước.

d. *Luật an ninh mạng Singapore*

Luật an ninh mạng đã được thông qua vào ngày 5 tháng 2 năm 2018 và nhận được sự đồng ý của Tổng thống vào ngày 2 tháng 3 năm 2018 để trở thành Đạo luật an toàn không gian mạng. Đạo luật thiết lập một khuôn khổ pháp lý cho việc giám sát và duy trì an ninh mạng quốc gia tại Singapore. Bốn mục tiêu chính của nó như sau.

Tăng cường bảo vệ cơ sở hạ tầng thông tin quan trọng (CII) chống lại các cuộc tấn công mạng. CII là hệ thống máy tính trực tiếp tham gia vào việc cung cấp các dịch vụ thiết yếu. Các cuộc tấn công trên mạng vào CII có thể ảnh hưởng đến nền kinh tế và xã hội. Đạo luật cung cấp khuôn khổ cho việc chỉ định CII và cung cấp cho chủ sở hữu CII một cách rõ ràng về nghĩa vụ của mình để chủ động bảo vệ CII khỏi các cuộc tấn công trên mạng. Điều này xây dựng khả năng khôi phục CII, bảo vệ nền kinh tế của Singapore và cách sống của người dân. Các ngành CII gồm có năng lượng, nước, ngân hàng và tài chính, y tế, giao thông vận tải (bao gồm đất đai, hàng hải và hàng không), thông tin liên lạc, truyền thông, dịch vụ bảo vệ và cấp cứu, và chính phủ.

Ủy quyền cho cơ quan an ninh mạng, CSA, ngăn chặn và ứng phó với các mối đe dọa và sự cố về an ninh mạng. Đạo luật trao quyền cho ủy viên an ninh không gian mạng điều tra các mối đe dọa an ninh mạng và các sự cố để xác định tác động của chúng và ngăn chặn các sự cố nguy hiểm hoặc sự cố không an toàn nảy sinh. Các quyền hạn có thể được hiệu chỉnh theo mức độ nghiêm trọng của mối đe dọa an ninh mạng hoặc sự cố và các biện pháp cần thiết để ứng phó. Điều này đảm bảo với người dân Singapore rằng chính phủ có thể đáp ứng hiệu quả các mối đe dọa an ninh mạng và giữ an toàn cho Singapore.

Luật này cũng thiết lập một khuôn khổ để chia sẻ thông tin an ninh mạng. Đạo luật cũng tạo điều kiện chia sẻ thông tin và điều quan trọng là thông tin kịp thời giúp chính phủ và chủ sở hữu hệ thống máy tính xác định các lỗ hổng và ngăn chặn sự cố mạng hiệu quả hơn. Đạo luật cung cấp một khuôn khổ cho CSA để yêu cầu thông tin, và để bảo vệ và chia sẻ thông tin đó.

Thiết lập khung cấp phép thuận tiện cho các nhà cung cấp dịch vụ bảo mật mạng. CSA sử dụng phương pháp tiếp cận đơn giản để chỉ cấp phép cho hai loại nhà cung cấp dịch vụ hiện nay, cụ thể là kiểm tra thâm nhập và quản lý trung tâm hoạt động an ninh (SOC). Hai dịch vụ này được ưu tiên vì các nhà cung cấp dịch vụ như vậy có quyền truy cập vào thông tin nhạy cảm từ khách hàng của họ. Các công ty này cũng tương đối phổ biến trong thị trường của Singapore và do đó có tác động đáng kể đến thực tiễn an ninh tổng thể. Khung cấp phép tìm cách cân bằng giữa nhu cầu bảo mật và sự phát triển của một hệ sinh thái an ninh mạng năng động.

## 7.4 Câu hỏi ôn tập

1. Trình bày các yêu cầu cơ bản với chính sách an toàn thông tin.
2. Giải trình mối liên quan giữa chính sách và pháp luật lên các yêu cầu an toàn thông tin.
3. Giải thích sự cần thiết của tiêu chuẩn an toàn thông tin.
4. Nêu tương quan giữa tiêu chuẩn an toàn thông tin và chính sách an toàn thông tin.
5. Trình bày các hành vi sử dụng máy tính và hệ thống mạng bị điều chỉnh bởi Luật hình sự của Việt Nam? Cho ví dụ minh hoạ.
6. Nêu các hành vi bị nghiêm cấm trong Luật giao dịch điện tử của Việt Nam?
7. Trình bày các điều kiện để đảm bảo an toàn cho chữ ký điện tử trong Luật giao dịch điện tử của Việt Nam?
8. Trình bày các hành vi bị nghiêm cấm trong Luật an toàn thông tin mạng và Luật an ninh mạng? Cho ví dụ minh hoạ.
9. Diễn giải các điều kiện hoạt động với các cơ quan/tổ chức theo quy định pháp luật Việt Nam và quốc tế?
10. Các yêu cầu về an toàn mà ứng dụng thương mại điện tử cần phải tuân thủ?
11. So sánh sự khác biệt trong cách tiếp cận vấn đề an toàn thông tin giữa các nước trong khu vực ASEAN?
12. Nêu sự khác biệt về vấn đề an toàn giữa EU, Mỹ và Trung Quốc.

# Tài liệu tham khảo


[1] Bộ Thông tin và Truyền thông, *V/v tăng cường công tác đảm bảo an toàn thông tin cho cổng/trang thông tin điện tử* (1790/BTTTT-VNCERT), 20/06/2011.

[2] Bộ Thông tin và Truyền thông, *Phân công nhiệm vụ trong việc triển khai thực hiện Quy hoạch phát triển an toàn thông tin số quốc gia đến năm 2010*, 21/06/2010.

[3] Hoàng Đăng Hải PGS. TSKH, *Quản lý an toàn thông tin*, Nhà xuất bản khoa học và kỹ thuật, ISBN 978-604-67-1062-2, 2018

[4] James Michael Stewart, Mike Chapple, Darril Gibson, *CISSP® Certified Information Systems Security*, Professional Study Guide, 2018 by John Wiley & Sons, Inc, ISBN: 978-1-119-47593-4

[5] John R Vacca, *Computer and Information Security Handbook*. 3rd ed, Elsevier Science, 2017.

[6] Michael E. Whitman and Herbert J. Mattord, *Management of Information Security*, Course Technology, Cengage Learning, 2010.

[7] Michael E. Whitman, Herbert J. Mattord, *Principles of information security, 4th edition*, Course Technology, Cengage Learning, 2012.

[8] Michael E. Whitman, Herbert J. Mattord, *Roadmap to Information Security: For CNTT and Infosec Managers*, Delmar Publishers Inc., 2011.

[9] Microsoft, Design Guidelines for Secure Web Applications, 2003

[10] Quốc hội Việt Nam, *Luật Công nghệ thông tin* (67/2006/QH11), 12/07/2006.

[11] Quốc hội Việt Nam, *Luật an toàn thông tin mạng* (86/2015/QH13), 2015

[12] Quốc hội Việt Nam, *Luật An ninh mạng* 24/ 2018/ QH14, 2018

[13] Sari Greene, *Security Policies and Procedures Principles and Practices*, Prentice Hall, 2005.

[14] Thủ tướng Chính phủ, V*/v tăng cường triển khai các hoạt động đảm bảo an toàn thông tin số* (897/CT-TTg), 10/06/2011.

[15] Thủ tướng Chính phủ, *Phê duyệt Quy hoạch phát triển an toàn thông tin số quốc gia đến năm 2020* (63/QĐ-TTg), 13/01/2010.