Bộ giáo trình những kiến thức cơ bản về công nghệ thông tin và truyền thông cho lãnh đạo trong cơ quan nhà nước

HỌC PHẦN 6

AN TOÀN, AN NINH THÔNG TIN VÀ MẠNG LƯỚI

Korea Information Security Agency

APCICT **Trung tâm đào tạo phát triển công nghệ thông tin và truyền thông Châu Á - Thái Bình Dương**

Bộ giáo trình những kiến thức cơ bản về CNTT&TT cho lãnh đạo trong cơ quan nhà nước

Học phần 6: An toàn, an ninh thông tin và mạng lưới

Trung tâm đào tạo công nghệ thông tin và truyền thông Châu Á Thái Bình Dương Trung (UN-APCICT)

Bonbudong, Tầng 3 Công viên công nghệ Songdo

7-50 Songdo-dong, Yeonsu-gu, Thành phố Incheon, Hàn Quốc

Điện thoại: +82 32 245 1700-02

Fax: +82 32 245 7712

E-mail: info@unapcict.org

http://www.unapcict.org

Thiết kế và trình bày: Scandinavian Publishing Co., Ltd

Xuất bản tại: Hàn Quốc

LỜI GIỚI THIỆU

Thế kỷ 21 đã đánh dấu sự tác động lẫn nhau của con người trên toàn cầu. Thế giới đang mở ra cơ hội cho hàng triệu người nhờ công nghệ mới, những thông tin và kiến thức thiết yếu được mở rộng đã cải thiện một cách đáng kể cuộc sống của con người và giúp giảm cảnh nghèo nàn. Điều này chỉ trở thành hiện thực khi có sự liên kết cùng với việc chia sẻ giá trị, cùng cam kết và thống nhất sự phát triển tổng thể và phù hợp.

Trong những năm gần đây, Châu Á Thái Bình Dương được biết đến như khu vực năng động nhất trong lĩnh vực công nghệ thông tin và truyền thông (ICT). Theo báo cáo của Liên minh Viễn thông Thế giới, khu vực này đã có trên 2 tỷ thuê bao điện thoại, trong đó có 1,4 tỷ thuê bao di động. Tinh đến năm 2008, chỉ riêng Ấn Độ và Trung Quốc đã chiếm ¼ số lượng thuê bao di động trên toàn thế giới. Khu vực Châu Á Thái Bình Dương được cho là chiếm 40% số lượng người sử dụng internet trên thế giới và đồng thời là thị trường băng rộng lớn nhất, với chiếm 39% thị trường toàn cầu.

Cùng với tốc độ phát triển nhanh của công nghệ, nhiều vấn đề được nhắc đến khi khoảng cách số biến mất. Nhưng điều đáng tiếc, khoảng cách số vẫn hiện hữu, thậm chí 5 năm sau khi Hội nghị thượng đỉnh thế giới về Xã hội thông tin (WSIS) diễn ra ở Geneva vào năm 2003, bất chấp sự phát triển ấn tượng của công nghệ và những cam kết của các nước lớn trong khu vực. Kết quả là truy nhập truyền thông cơ bản vẫn còn xa lạ với nhiều người, đặc biệt là những người nghèo.

Hơn 25 quốc gia trong khu vực gồm những nước đang phát triển, đã có gần 10 người sử dụng internet trên 100 dân, phần lớn tập trung ở các thành phố lớn. Trong khi đó ở một vài nước đã phát triển trong khu vực thì tỉ lệ rất cao với hơn 80 người sử dụng internet trên 100 dân. Sự chênh lệch về mức độ phổ cập băng rộng giữa các nước phát triển và đang phát triển vẫn còn là giữ một khoảng cách lớn.

Để giảm dần khoảng cách số và nhận diện đúng tiềm năng của ICT cho phát triển kinh tế xã hội trong khu vực, những nhà lập pháp ở các nước phát triển cần xây dựng các chính sách ưu tiên và khung điều chỉnh, chỉ định nguồn

quỹ, và tạo điều kiện cho xúc tiến đầu tư vào lĩnh vực công nghiệp ICT và nâng cao kỹ năng ICT cho công dân nước họ.

Trong Kế hoạch Hành động của WSIS có chỉ rõ, "… mỗi người sẽ có cơ hội tiếp cận những kỹ năng và kiến thức cần thiết để hiểu, thực hành và đạt được những lợi ích từ Xã hội Thông tin và Kinh tế Tri thức.". Trong phần cuối của kế hoạch này đã kêu gọi sự hợp tác quốc tế và khu vực trong những lĩnh vực có tiềm năng, đặc biệt nhấn mạnh vào việc tạo tập một số lượng lớn các chuyên gia ICT.

Để hỗ trợ tốt cho lời kêu gọi từ Kế hoạch hành động của WSIS, APCICT đã xây dựng chương trình giảng dạy đầy đủ về ICT – Học thuật ICT cần thiết cho nhà lãnh đạo trực thuộc cơ quan nhà nước. Chương trình này bao gồm 8 phần có liên kết chặt chẽ với nhau, với mục tiêu truyền đạt những kiến thức và kinh nghiệm cần thiết giúp các nhà lập pháp xây dựng và thi hành sáng kiến ICT hiệu quả hơn.

APCICT là một trong 5 học viện của Ủy ban Kinh tế Xã hội Liên hợp quốc Châu Á Thái Bình Dương. APCICT xúc tiến chương trình phát triển kinh tế xã hội phù hợp và toàn diện ở Châu Á Thái Bình Dương thông qua việc phân tích, chuẩn hóa, khai thác tiềm năng, hợp tác khu vực và chia sẻ kiến thức. Trong quá trình hợp tác với các cơ quan Liên hợp quốc khác, các tổ chức quốc tế, các quốc gia và những tổ chức liên quan, ESCAP, đại diện là APCICT, được giao nhiệm vụ hỗ trợ việc sử dụng, cải tiến và dịch thuật các bài giảng cho các quốc gia khác nhau, phù hợp với các trình độ trung và cao cấp của các nhân viên trong cơ quan nhà nước, với mục đích đưa kỹ năng và kiến thức thu thập được làm gia tăng những lợi ích từ ICT và thiết lập những hành động cụ thể để đạt được mục tiêu phát triển.

Noeleen Heyzer

TL. Tổng Thư ký Liên hợp quốc

Và Giám đốc điều hành của ESCAP

LỜI TỰA

Chặng đường phát triển của bộ giáo trình những kiến thức cơ bản về công nghệ thông tin và truyền thông (CNTT&TT) cho lãnh đạo trong cơ quan nhà nước thực sự là một kinh nghiệm mang tính trí tuệ cao. Bộ giáo trình không chỉ phục vụ cho việc xây dựng các kỹ năng CNTT&TT, mà còn mở đường cho một phương thức mới về xây dựng chương trình giảng dạy - thông qua sự hợp tác của các thành viên và tự chủ về quy trình.

Bộ giáo trình là một chương trình mang tính chiến lược của APCICT, phát triển trên cơ sở kết quả khảo sát đánh giá nhu cầu một cách toàn diện được tiến hành trên 20 nước trong khu vực và sự tham khảo ý kiến của các nhân viên thuộc cơ quan nhà nước, thành viên các cơ quan phát triển quốc tế, các viện hàn lâm và cơ sở giáo dục; những nghiên cứu và phân tích kỹ lưỡng về điểm mạnh và điểm yếu của giáo trình đào tạo; thông tin phản hồi từ những người tham gia xây dựng chuỗi bài giảng của APCICT – tổ chức các buổi hội thảo khu vực và quốc gia liên quan đến nội dung bài giảng và các phương pháp đào tạo khoa học; và sự trao đổi góp ý thẳng thắn của các chuyên gia hàng đầu trong các lĩnh vực ICT phục vụ phát triển. Các hội thảo về giáo trình diễn ra ở các khu vực thu được những lợi ích vô giá từ các hoạt động trao đổi kinh nghiệm và kiến thức giữa những người tham dự đến từ các quốc gia khác nhau. Đó là một quy trình để các tác giả xây dựng nội dung.

Việc xây dựng 8 học phần trong bộ giáo trình đánh dấu một sự khởi đầu quan trọng trong việc nâng cao sự hợp tác ở hiện tại và xây dựng các mối liên hệ mới nhằm phát triển các kỹ năng thiết lập chính sách phát triển CNTT&TT khắp khu vực. APCICT cam kết cung cấp sự hỗ trợ kỹ thuật trong việc giới thiệu bộ giáo trình quốc gia như một mục tiêu chính hướng tới việc đảm bảo rằng bộ giáo trình sẽ được phổ biến tới tất cả những nhà lập pháp. APCICT cũng đang xúc tiến một cách chặt chẽ với một số viện đào tạo trong khu vực và quốc tế, những tổ chức có mối quan hệ mật thiết với cơ quan nhà nước cấp trung ương và địa phương để cải tiến, dịch thuật và truyền đạt các nội dung của Giáo trình tới những quốc gia có nhu cầu. APCICT đang tiếp tục mở rộng hơn nữa về đối tượng tham gia nghiên cứu giáo trình hiện tại và kế hoạch phát triển một giáo trình mới.

Hơn nữa, APCICT đang xúc tiến nhiều kênh để đảm bảo rằng nội dung Giáo trình đến được nhiều người học nhất trong khu vực. Ngoài phương thức học trực tiếp thông qua các tổ chức lớp học ở các khu vực và quốc gia, APCICT cũng tổ chức các lớp học ảo (AVA), phòng học trực tuyến cho phép những học viên tham gia bài giảng ngay tại chỗ làm việc của họ. AVA đảm bảo rằng tất cả các phần bài giảng và tài liệu đi kèm cũng như bản trình chiếu và bài tập tình huống dễ dàng được truy nhập trực tuyến và tải xuống, sử dụng lại, cải tiến và bản địa hóa, và nó bao gồm nhiều tính năng khác nhau như bài giảng ảo, công cụ quản lý học tập, công cụ phát triển nội dung và chứng chỉ.

Việc xuất bản và giới thiệu 8 học phần của bộ giáo trình thông qua các buổi hội thảo khu vực, tiểu khu vực, quốc gia có sự tận tâm cống hiến, tham gia tích cực của nhiều cá nhân và tổ chức. Tôi muốn nhân cơ hội này để bày tỏ lòng cảm ơn những nỗ lực và kết quả đạt được của nhóm cộng tác và các đối tác từ các Bộ, ngành, học viện, và các tổ chức khu vực và quốc gia đã tham gia hội thảo về bộ giáo trình. Họ không chỉ cũng cung cấp những thông tin đầu vào có giá trị, phục vụ nội dung của bài giảng, mà quan trọng hơn, họ đã trở thành những người ủng hộ việc truyền đạt bộ giáo trình trên đất nước mình, tạo ra kết quả là những thỏa thuận chính thức giữa APCICT và một số viện đối tác của các quốc gia và trong khu vực để cải tiến và phát hành bài giảng giáo trình chính thức cho đất nước họ.

Tôi cũng muốn gửi lời cảm ơn đặc biệt cho những nỗ lực cống hiến của nhiều cá nhân nổi bật, những người đã tạo nên thành quả cho bài giảng này. Họ là Shahid Akhtar Cố Vấn Dự án Giáo trình; Patricia Arinto, Biên tập; Christine, Quản lý xuất bản; toàn bộ tác giả bộ giáo trình; và những nhóm APCICT.

Chúng tôi hy vọng rằng bộ giáo trình sẽ giúp các quốc gia thu hẹp được những hạn chế của nguồn nhân lực CNTT&TT, xóa bỏ những rào cản nhận thức về CNTT&TT, và xúc tiến ứng dụng CNTT&TT trong việc thúc đẩy phát triển kinh tế xã hội và đạt được mục tiêu phát triển thiên nhiên kỷ.

Hyeun – Suk Rhee

Giám đốc UN-APCICT

VỀ CHUỖI HỌC PHẦN

Trong kỷ nguyên thông tin ngày nay, việc truy cập thông tin một cách dễ dàng đang làm thay đổi cách chúng ta sống, làm việc và giải trí. Nền kinh tế số - còn được gọi là kinh tế tri thức, kinh tế mạng hay kinh tế mới, được mô tả như một sự chuyển tiếp từ sản xuất hàng hóa sang tạo lập ý tưởng. Công nghệ thông tin và truyền thông đang đóng một vai trò quan trọng và toàn diện trên mọi mặt của kinh tế xã hội.

Như một kết quả, chính phủ trên khắp thế giới đang quan tâm nhiều hơn tới CNTT&TT trong sự phát triển quốc gia. Đối với các nước, phát triển CNTT&TT không chỉ phát triển về công nghiệp CNTT&TT là một lĩnh vực của nền kinh tế mà còn bao gồm cả việc ứng dụng CNTT&TT trong hoạt động kinh tế, xã hội và chính trị.

Tuy nhiên, giữa những khó khăn mà chính phủ các nước phải đối mặt trong việc thi hành các chính sách CNTT&TT, những nhà lập pháp thường không nắm rõ về mặt công nghệ đang sử dụng cho sự phát triển quốc gia. Cho đến khi không thể điều chỉnh được những điều họ không hiểu, nhiều nhà lập pháp né tránh tạo lập các chính sách về CNTT&TT. Nhưng chỉ quan tâm tới công nghệ mà không tạo lập các chính sách thì cũng là một sai lầm vì những nhà công nghệ thường ít có kiến thức về thi hành những công nghệ họ đang phát triển hoặc sử dụng.

Bộ giáo trình những kiến thức cơ bản về công nghệ thông tin và truyền thông (CNTT&TT) cho lãnh đạo trong cơ quan nhà nước do Trung tâm Đào tạo Phát triển Công nghệ thông tin và Truyền thông Liên hợp quốc và Châu Á Thái Bình Dương (UN-APCICT) xây dựng nhằm phục vụ cho:

1. Các nhà hoạch định chính sách về CNTT&TT cả ở mức độ quốc gia và địa phương;

2. Quan chức chính phủ chịu trách nhiệm về phát triển và thi hành các ứng dụng của CNTT&TT; và

3. Những nhà quản lý trong lĩnh vực công đang tìm kiếm chức danh quản lý dự án về CNTT&TT.

Bộ giáo trình hướng đến những vấn đề liên quan tới CNTT&TT phục vụ phát triển trên cả khía cạnh chính sách và công nghệ. Mục đích cốt yếu của giáo trình CNTT&TT không tập trung vào kỹ thuật mà truyền đạt sự hiểu biết về những điều công nghệ số có khả năng hoặc đang hướng tới, tác động tới như thế nào trong việc hoạch định chính sách. Các chủ đề trong bài giảng được thiết kế dựa trên phân tích nhu cầu và khảo sát những chương trình đào tạo trên khắp thế giới.

Học phần được cấu tạo theo cách mà người học có thể tự học một cách độc lập hoặc bài giảng cho một khóa học. Học phần vừa mang tính chất riêng lẻ nhưng cũng liên kết với những chủ đề và tình huống thảo luận trong phần khác của chuỗi. Mục tiêu là tạo được sự thống nhất ở tất cả các phầncác phần.

Mỗi phần bắt đầu với việc trình bày một chủ đề và kết quả mà người đọc sẽ thu được. Nội dung các phần được chia thành các mục bao gồm bài tập và tình huống để giúp hiểu sâu hơn những nội dung chính. Bài tập có thể được thực hiện bởi từng cá nhân hoặc một nhóm học viên. Biểu đồ và bảng biểu được cung cấp để minh họa những nội dung của buổi thảo luận. Tài liệu tham khảo được liệt kê để cho người đọc có thể tự tìm hiểu sâu hơn về bài giảng.

Việc sử dụng CNTT&TT phục vụ phát triển rất đa dạng, trong một vài tình huống hoặc thí dụ ở bài giảng có thể xuất hiện những mâu thuẫn. Đây là điều đáng tiếc. Đó cũng là sự kích thích và thách thức của quá trình rèn luyện mới và cũng là triển vọng khi tất cả các nước bắt đầu khai tiềm năng của CNTT&TT như công cụ phát triển.

Hỗ trợ chuỗi học phần còn có một phương thức học trực tuyến – Học viện ảo ACICT (AVA – http://www.unapcict.org/academy) – với phòng học ảo sẽ chiếu bản trình bày của người dạy dưới dạng video và Power Point của học phần.

Ngoài ra, APCICT đã phát triển một kênh cho phát triển CNTT&TT (e-Co Hub – http://www.unapcict.org/ecohub), một địa chỉ trực tuyến dành cho những học viên phát triển CNTT&TT và những nhà lập pháp nâng cao kinh nghiệm học tập. E-Co Hub cho phép truy cập những kiến thức về các chủ đề khác nhau của phát triển CNTT&TT và cung cấp một giao diện chia sẻ kiến thức và kinh nghiệm, và hợp tác trong việc nâng cao CNTT&TT phục vụ phát triển.

HỌC PHẦN 6

Trong thời đại thông tin, tin tức là một tài sản được bảo vệ và những nhà hoạch định chính sách cần nắm được bảo mật thông tin là gì và làm thế nào để chống lại các xâm phạm và rỏ rỉ thông tin. Phần này giới thiệu tổng quan về nhu cầu bảo mật thông tin, xu hướng và các vấn đề bảo mật thông tin, cũng như quá trình xây dựng chiến lược bảo mật thông tin.

Mục tiêu của học phần

Học phần nhằm đạt được các mục tiêu:

1. Làm sáng tỏ khái niệm an toàn, an ninh thông tin và các khái niệm liên quan;
2. Mô tả những thách thức đối với bảo mật thông tin và làm thế nào để có thể xác định chúng;
3. Thảo luận về nhu cầu thiết lập và thực hiện chính sách an ninh thông tin, cũng như sự thay đổi phát triển của chính sách an ninh thông tin; và
4. Giới thiệu tổng quan về các tiêu chuẩn bảo đảm an toàn, an ninh thông tin được sử dụng ở một số quốc gia cũng như các tổ chức an ninh thông tin quốc tế.

Kết quả thu được

Sau khi nghiên cứu xong học phần này, người đọc có thể:

1. Định nghĩa an toàn, an ninh thông tin và các khái niệm liên quan;
2. Nhận định những thách thức đối với an ninh thông tin;
3. Đánh giá chính sách an ninh thông tin hiện có theo các tiêu chuẩn quốc tế về bảo đảm an toàn, an ninh thông tin; và
4. Xây dựng hoặc đưa ra các khuyến nghị về chính sách an ninh thông tin thích hợp.

MỤC LỤC

DANH MỤC HÌNH VẼ

DANH MỤC BẢNG BIỂU

DANH MỤC TỪ VIẾT TẮT

APCERT	Asia-Pacific Computer Emergency Response Team
APCICT	Asian and Pacific Training Centre for Information and Communication Technology for Development
APEC	Asia-Pacific Economic Cooperation
BPM	Baseline Protection Manual
BSI	British Standards Institution
BSI	Bundesamt fűr Sicherheit in der Informationstechnik, Germany
CAP	Certificate Authorizing Participant
CC	Common Criteria
CCP	Certificate Consuming Participant
CCRA	Common Criteria Recognition Arrangement
CECC	Council of Europe Convention on Cybercrime
CERT	Computer Emergency Response Team
CERT/CC	Computer Emergency Response Team Coordination Center
CIIP	Critical Information Infrastructure Protection
CISA	Certified Information Systems Auditor
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CM	Configuration Management
CSEA	Cyber Security Enhancement Act
CSIRT	Computer Security Incident Response Team
DID	Defense-In-Depth
DNS	Domain Name Server
DoS	Denial-of-Service
ECPA	Electronic Communications Privacy Act
EGC	European Government Computer Emergency Response Team
ENISA	European Network and Information Security Agency
ERM	Enterprise Risk Management
ESCAP	Economic and Social Commission for Asia and the Pacific
ESM	Enterprise Security Management
EU	European Union
FEMA	Federal Emergency Management Agency
FIRST	Forum of Incident Response and Security Teams

FISMA	Federal Information Security Management Act
FOI	Freedom of Information
GCA	Global Cybersecurity Agenda
HTTP	Hypertext Transfer Protocol
ICT	Information and Communication Technology
ICTD	Information and Communication Technology for Development
IDS	Intrusion Detection System
IGF	Internet Governance Forum
IM	Instant-Messaging
IPS	Intrusion Prevention System
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO/IEC	International Organization for Standardization and International Electrotechnical Commission
ISP	Internet Service Provider
ISP/NSP	Internet and Network Service Provider
IT	Information Technology
ITU	International Telecommunication Union
ITU-D	International Telecommunication Union Development Sector
ITU-R	International Telecommunication Union Radiocommunication Sector
ITU-T	International Telecommunication Union Standardization Sector
KISA	Korea Information Security Agency
MIC	Ministry of Information and Communication, Republic of Korea
NIS	Network and Information Security
NISC	National Information Security Center, Japan
NIST	National Institute of Standards and Technology, USA
OECD	Organisation for Economic Co-operation and Development
OMB	Office of Management and Budget, USA
OTP	One-Time Passwords
PC	Personal Computer
PP	Protection Profile
PSG	Permanent Stakeholders Group
RFID	Radio Frequency Identification
SAC	Security Assurance Component
SFR	Security Functional Requirement

SME	Small and Medium Enterprise
ST	Security Target
TEL	Telecommunication and Information Working Group
TOE	Target of Evaluation
TSF	TOE Security Functions
UK	United Kingdom
UN	United Nations
US	United States
USA	United States of America
WPISP	Working Party on information Security and Privacy
WSIS	World Summit on the Information Society

1. NHU CẦU VỀ AN NINH THÔNG TIN

Phần này nhằm mục đích:

. Giải thích khái niệm thông tin và an ninh thông tin; và

. Mô tả những tiêu chuẩn được áp dụng cho các hoạt động an ninh thông tin.

Cuộc sống con người ngày nay phụ thuộc nhiều vào công nghệ thông tin và truyền thông (ICT). Điều này khiến cho các cá nhân, tổ chức và các quốc gia dễ bị tấn công qua các hệ thống thông tin, như các hình thức hacking (thâm nhập trái phép), cyberterrorism (khủng bố mạng), cybercrime (tội phạm mạng) cũng như các hình thức tương tự. Một số cá nhân và tổ chức được trang bị để có thể đối phó với các cuộc tấn công như vậy. Chính phủ có vai trò quan trọng trong công tác đảm bảo an ninh thông tin thông qua việc mở rộng cơ sở hạ tầng thông tin – truyền thông và thiết lập các hệ thống bảo vệ chống lại những nguy cơ đối với an ninh thông tin.

1.1. Các khái niệm cơ bản trong An ninh thông tin

"Thông tin" là gì?

Thông thường, thông tin được định nghĩa là kết quả của hoạt động trí óc; đó là sản phẩm vô hình, được truyền tải qua các phương tiện truyền thông. Trong lĩnh vực ICT, thông tin là kết quả của quá trình xử lý, thao tác và tổ chức dữ liệu, có thể đơn giản như việc thu thập số liệu thực tế.

Trong phạm vi của An ninh thông tin, thông tin được định nghĩa như một "tài sản", có giá trị do đó nên được bảo vệ. Học phần này sẽ sử dụng định nghĩa về thông tin và an ninh thông theo tiêu chuẩn ISO/IEC 27001.

Ngày nay, giá trị của thông tin phản ánh sự chuyển đổi từ một xã hội nông nghiệp sang xã hội công nghiệp và cuối cùng là xã hội hướng thông tin (information-oriented society). Trong xã hội nông nghiệp, đất đai là tài sản quan

trọng nhất và quốc gia nào có sản lượng lương thực nhiều nhất sẽ chiếm được lợi thế cạnh tranh. Trong xã hội công nghiệp, với sức mạnh tư bản, như có được các nguồn dự trữ dầu mỏ là nhân tố chủ chốt của khả năng cạnh tranh. Trong xã hội hướng thông tin và tri thức, thông tin là tài sản quan trọng nhất và năng lực thu thập, phân tích và sử dụng thông tin là lợi thế cạnh tranh cho bất kỳ quốc gia nào.

Với viễn cảnh chuyển đổi từ giá trị tài sản hữu hình sang giá trị tài sản thông tin, có một sự đồng thuận cao đó là thông tin cần được bảo vệ. Bản thân thông tin có giá trị cao hơn phương tiện lưu trữ chúng. Bảng 1 sẽ đối chiếu thông tin với các tài sản hữu hình.

Bảng 1. Sự so sánh thông tin với các tài sản hữu hình

Đặc điểm	Tài sản thông tin	Tài sản hữu hình
Hình thái – Sự duy trì	Không có hình dạng vật lý và có thể linh hoạt	Có hình dạng vật lý
Giá trị - Tính biến đổi	Có giá trị cao hơn khi được xử lý và phối hợp	Tổng giá trị là sự tổng hợp các giá trị thành phần
Sự chia sẻ	Không giới hạn việc tái sản xuất các tài sản thông tin và mọi người có thể chia sẻ giá trị	Việc tái sản xuất là không thể; khi tái sản xuất, giá trị của tài sản sẽ bị giảm đi
Phương tiện truyền thông – Tính phụ thuộc	Cần được phát tán thông qua các phương tiện truyền thông	Có thể phân phát một cách độc lập (nhờ hình thái vật lý của tài sản)

Như chúng ta thấy ở bảng 1, tài sản thông tin về cơ bản khác với tài sản hữu hình. Chính vì vậy, thông tin có thể bị tấn công bởi những loại hình rủi ro khác.

Các mối hiểm họa đối với tài sản thông tin

Khi giá trị của tài sản thông tin nâng lên, nhu cầu kiểm soát cũng như truy nhập thông tin giữa con người với nhau gia tăng. Các nhóm hình thành và sử dụng thông tin với nhiều mục tiêu khác nhau, và một số cố gắng để giành được

thông tin bằng bất kỳ cách thức nào. Nó bao gồm thâp nhập trái phép (hacking), đánh cắp (piracy) và phá hủy các hệ thống thông tin thông qua virus máy tính và các hình thức khác. Những hiểm họa đi kèm với quá trình tin học hóa được thảo luận trong phần 2 của học phần này.

Mặt trái của môi trường hướng thông tin bao gồm các vấn đề sau:

Gia tăng những hành vi ứng xử trái với quy tắc nảy sinh từ tình trạng nặc danh – ICT có thể được sử dụng để duy trì tình trạng nặc danh, tạo điều kiện dễ dàng cho các cá nhân dàn xếp những hành vi phạm tội và ứng xử trái quy tắc, bao gồm cả việc chiếm dụng thông tin một cách bất hợp pháp.

Xung đột quyền kiểm soát và sở hữu thông tin – Sự phức tạp về quyền kiểm soát và sở hữu thông tin ngày một tăng lên cùng với việc mở rộng quá trình tin học hóa. Ví dụ như khi chính phủ nỗ lực xây dựng một cơ sở dữ liệu người dân dưới mô hình chính phủ điện tử, một số bộ phận có phàn nàn về khả năng xâm phạm bí mật đời tư từ việc phơi bày các thông tin cá nhân cho người khác.

Khoảng cách thông tin và mức độ giàu có giữa các tầng lớp, quốc gia – Kích thước của vật chứa đựng tài sản thông tin có thể biểu thị sự giàu có trong xã hội hướng thông tin/tri thức. Các quốc gia phát triển có khả năng sản xuất ra thông tin và kiếm lợi từ việc bán thông tin như các sản phẩm hàng hóa. Ngược lại, các nước nghèo thông tin, có nhu cầu đầu tư lớn chỉ có thể truy cập thông tin.

Tình trạng phơi bày thông tin tăng lên bắt nguồn từ các hệ thống mạng tiên tiến – Xã hội hướng thông tin/tri thức là một xã hội mạng lưới. Cả thế giới được kết nối như một hệ thống mạng duy nhất, điều này có nghĩa là sự yếu kém của một phần nào đó trong mạng lưới sẽ tác động xấu đến các phần còn lại.

An ninh thông tin là gì?

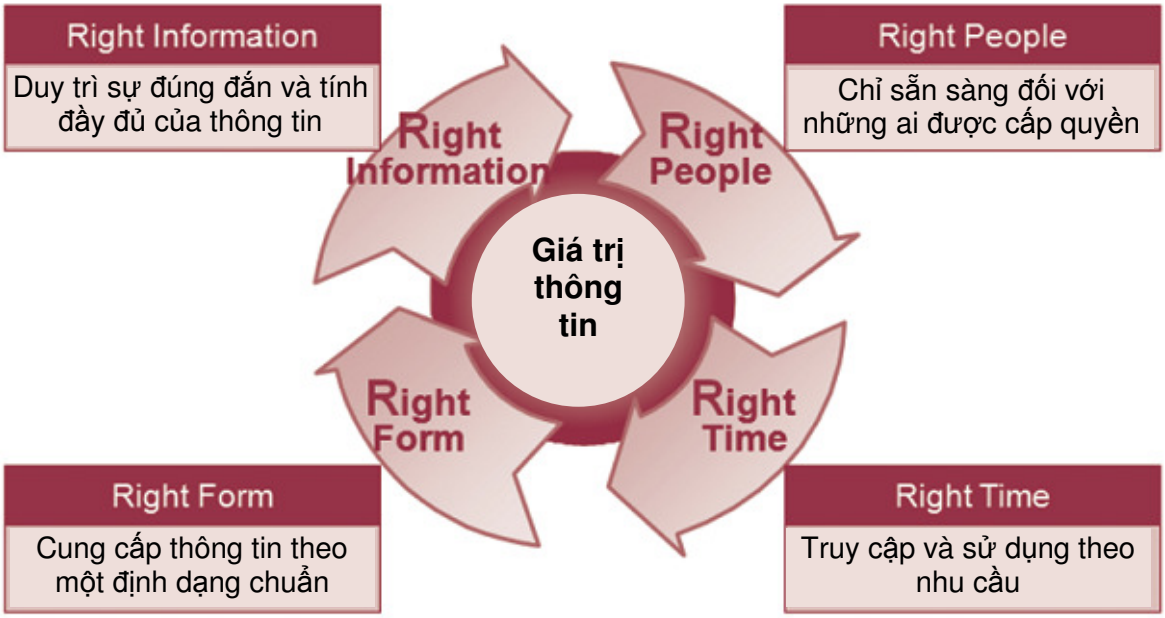
Đáp lại những cố gắng giành lấy thông tin một cách bất hợp pháp, con người đang nỗ lực để ngăn chặn tội phạm liên quan đến thông tin hoặc giảm thiểu thiệt hại do tội phạm gây ra. Điều này được gọi là an ninh thông tin.

Diễn đạt một cách đơn giản, an ninh thông tin là việc nhận biết giá trị của thông tin và bảo vệ nó.

4R trong an ninh thông tin

Bộ 4R trong an ninh thông tin đó là Right Information (thông tin đúng), Right People (con người đúng), Right Time (thời gian đúng) và Right Form (định dạng đúng). Kiểm soát toàn bộ 4R này là cách thức tốt nhất để kiểm soát và duy trì giá trị của thông tin.

Hình 1. 4R trong an ninh thông tin



"Right Information" thể hiện sự đúng đắn và tính chất đầy đủ của thông tin, đảm bảo tính toàn vẹn của thông tin.

"Right People" có nghĩa là thông tin chỉ sẵn sàng đối với những người được cấp quyền, đảm bảo tính bí mật của thông tin.

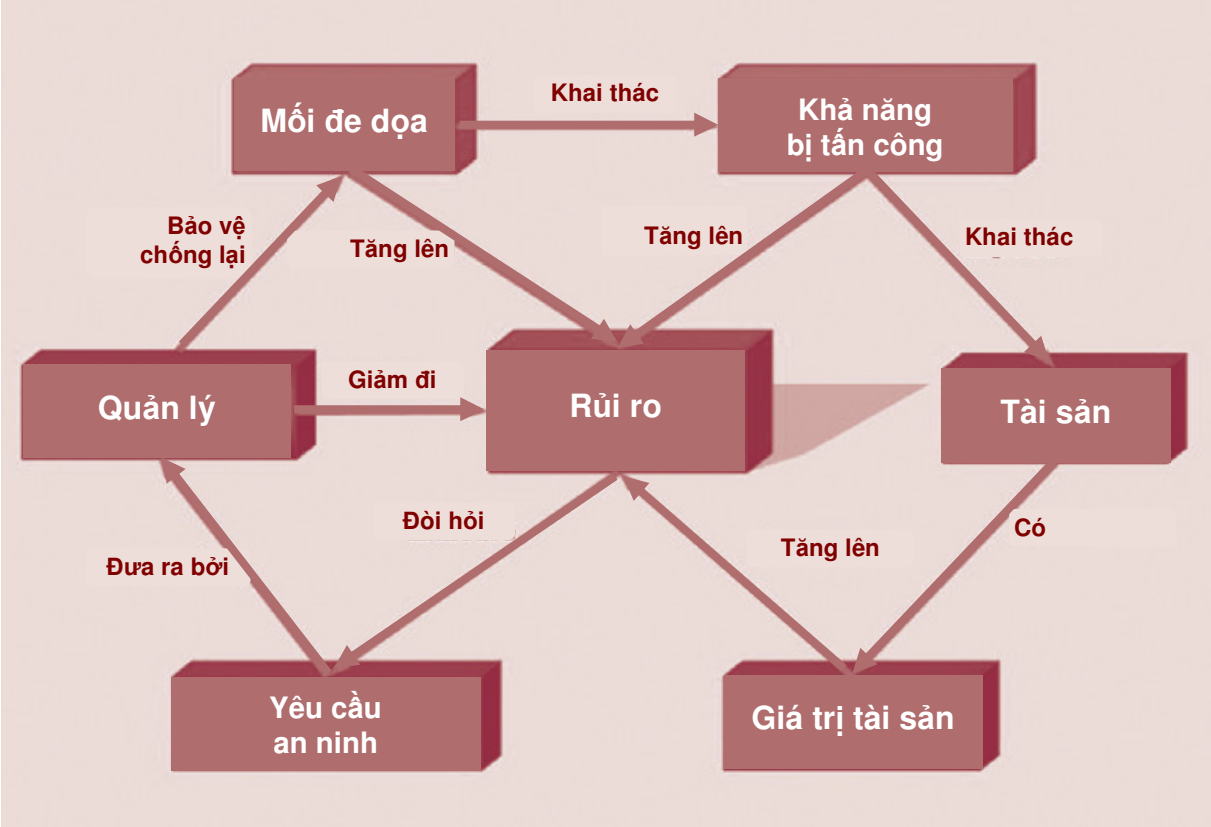
"Right Time" thể hiện khả năng có thể truy cập và tính khả dụng của thông tin theo yêu cầu của thực thể có thẩm quyền. Điều này đảm bảo tính sẵn sàng của thông tin.

"Right Form" thể hiện việc cung cấp thông tin theo một định dạng chuẩn.

Để bảo đảm an ninh thông tin, mô hình 4R phải được áp dụng một cách đúng đắn. Điều này có nghĩa là tính bí mật, tính toàn vẹn và tính sẵn sàng cần được giám sát trong quá trình quản lý thông tin.

An ninh thông tin cũng yêu cầu sự am hiểu rõ ràng về giá trị của tài sản thông tin, cũng như khả năng bị xâm phạm và những mối đe dọa tương ứng. Vấn đề này được biết đến như công tác quản lý rủi ro. Hình 2 thể hiện sự tương quan giữa tài sản thông tin và rủi ro.

Hình 2. Mối tương quan giữa rủi ro và tài sản thông tin



Rủi ro được xác định thông qua giá trị tài sản, các mối đe dọa và khả năng bị xâm phạm. Công thức như sau:

Rủi ro = $\int$ (Giá trị tài sản, Các mối đe dọa, Khả năng bị xâm phạm)

Rủi ro tỉ lệ thuận với giá trị tài sản, các mối đe dọa và khả năng bị xâm phạm. Do đó, rủi ro có thể bị tăng lên hay giảm đi thông qua việc thay đổi quy mô giá trị tài sản, các mối đe dọa và khả năng bị xâm phạm. Điều này có thể thực hiện thông qua công tác quản lý rủi ro.

Các phương pháp quản lý rủi ro bao gồm:

Thu hẹp rủi ro (giảm nhẹ rủi ro) – Phương pháp này được thực hiện khi khả năng xảy ra của các mối đe dọa/khả năng bị xâm hại cao nhưng tác động của chúng thấp. Nó đòi hỏi sự am hiểu các mối đe dọa và khả năng bị xâm phạm là

gì, thay đổi hay giảm thiểu chúng, và việc triển khai một biện pháp đối phó. Tuy vậy, việc thu hẹp rủi ro không làm giảm giá trị của rủi ro tới mức '0'.

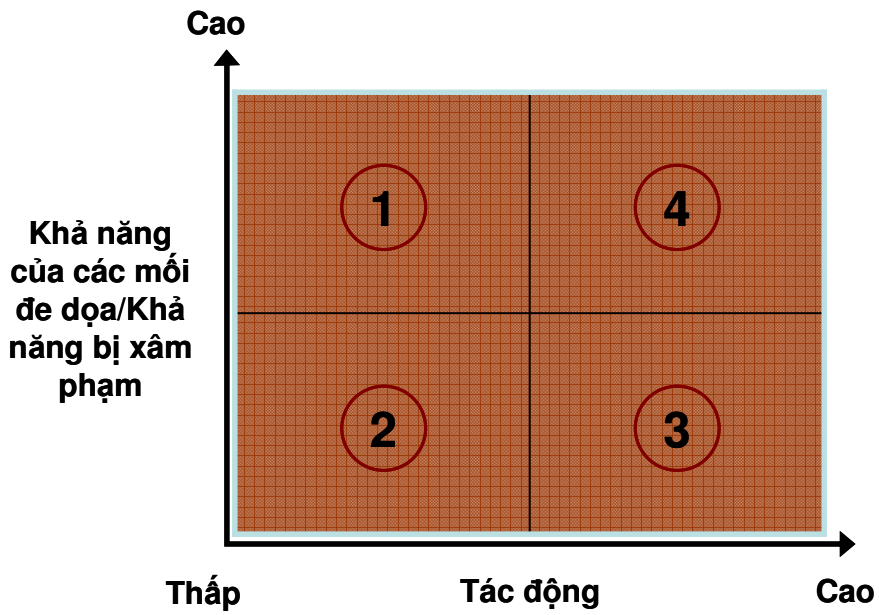
Chấp nhận rủi ro – Phương pháp này được thực hiện khi khả năng xảy ra của các mối đe dọa/khả năng bị xâm hại thấp và ảnh hưởng của chúng có vẻ thấp hoặc có thể chấp nhận được.

Di chuyển rủi ro – Nếu rủi ro ở mức quá cao hoặc tổ chức không có khả năng chuẩn bị các giải pháp kiểm soát cần thiết thì rủi ro có thể được di chuyển ra bên ngoài tổ chức. Một ví dụ đó là áp dụng một chính sách bảo hiểm.

Tránh xa rủi ro – Nếu các mối đe doa và khả năng bị xâm phạm có khả năng cao xảy ra và tác động của chúng cũng ở mức rất cao thì phương pháp tốt nhất là tránh xa rủi ro, ví dụ như bằng cách thuê ngoài đội ngũ cũng như trang thiết bị xử lý dữ liệu.

Hình 3 là một biểu đồ minh họa cho bốn phương pháp quản lý rủi ro. Trong hình này, góc phân tư số '1' là *Thu hẹp rủi ro*, góc phần tư số '2' là *Chấp nhận rủi ro*, góc phần tư số '3' là *Di chuyển rủi ro*, và góc phần tư số '4' là *Tránh xa rủi ro*.

Hình 3. Các phương pháp quản lý rủi ro



Nhân tố chính trong việc xem xét lựa chọn phương pháp quản lý rủi ro thích hợp đó là mối quan hệ chi phi – hiệu quả. Công tác phân tích chi phí – hiệu

quả nên được tiến hành trước khi thiết lập các phương án thu hẹp rủi ro, chấp nhận rủi ro, di chuyển rủi ro hay tránh xa rủi ro.

1.2. Các tiêu chuẩn cho hoạt động an ninh thông tin

Các hoạt động an ninh thông tin không thể thực hiện một cách hiệu quả mà thiếu một kế hoạch vật chất và kỹ thuật cũng như quản trị một cách đồng bộ.

Nhiều tổ chức có những tiêu chuẩn khuyến nghị cho các hoạt động an ninh thông tin. Tiêu biểu là các yêu cầu an ninh thông tin của Ủy ban Kỹ thuật chung (ISO/IEC) giữa Tổ chức Tiêu chuẩn hóa Quốc tế (International Organization for Standardization - ISO) và Hội đồng Kỹ thuật điện Quốc tế (International Electrotechnical Commission - IEC); các tiêu chuẩn đánh giá CISA (Certified Information Systems Auditor) và CISSP (Certified Information Systems Security Professional) của Hiệp hội Điều hanh và Kiểm toán hệ thống thông tin ISACA (Information Systems Audit and Control Association). Các tiêu chuẩn này khuyến nghị cho các hoạt động an ninh thông tin đồng nhất, như xây dựng một chính sách an ninh thông tin, xây dựng và điều hành một tổ chức an ninh thông tin, quản lý nguồn nhân lực, quản lý an ninh các yếu tố vật chất, quản lý an ninh các yếu tố kỹ thuật, quản lý hoạt động kinh doanh liên tục và kiểm toán hệ thống.

Bảng 2 liệt kê các tiêu chuẩn liên quan tới lĩnh vực an ninh thông tin.

Bảng 2. Các tiêu chuẩn liên quan và phạm vi của an ninh thông tin

Phạm vi an ninh thông tin	ISO/IEC 27001	CISA	CISSP
Quản trị điều hành	Chính sách an ninh	Quản trị IT	Thực tiễn quản lý an ninh Mô hình và kiến trúc an ninh
	Tổ chức về an ninh thông tin	Quản trị IT	
	Quản lý tài sản	Bảo vệ tài sản thông tin	Thực tiễn quản lý an ninh
	An ninh nguồn nhân lực		

	Quản lý các tình huống bất ngờ liên quan tới an ninh thông tin	Khôi phục các thảm họa và tính liên tục của công việc kinh doanh	Lập kế hoạch khôi phục thảm họa và lập kế hoạch duy trì tính liên tục của công việc kinh doanh
	Quản lý tính liên tục trong công việc kinh doanh	Khôi phục các thảm họa và tính liên tục của công việc kinh doanh	Lập kế hoạch khôi phục thảm họa và lập kế hoạch duy trì tính liên tục của công việc kinh doanh
	Sự tuân thủ	Quá trình kiểm toán hệ thống thông tin	Luật lệ, công tác điều tra và các nội quy
Các yếu tố vật chất	An ninh môi trường và các yếu tổ vật chất		An ninh các yếu tố vật chất
Các yếu tố kỹ thuật	Quản lý điều hành và truyền thông	Quản lý vòng đời cơ sở hạ tầng và các hệ thống	Công nghệ mã hóa An ninh mạng lưới và truyền thông An ninh điều hành
	Quản trị truy nhập		
	Bảo trì và phát triển, thu nhận các hệ thống thông tin	Hỗ trợ và giao phát dịch vụ IT	

Tiêu chuẩn ISO/IEC27001[1] tập trung vào an ninh quản trị. Cụ thể, nó nhấn mạnh công tác kiểm toán hoạt động và tài liệu như hành vi quản trị và việc giám sát các quy tắc cũng như chính sách/định hướng. Tiếp đó, việc xác nhận và các biện pháp đối phó được yêu cầu đưa ra bởi nhà quản trị. Do vậy, ISO/IEC27001 cố gắng xác định những điểm yếu trong trang thiết bị, các hệ thống an ninh và những yếu tố tương tự trong một đường lối quản trị.

Ngược lại, không có đề cập nào về an ninh các yếu tổ vật chất và nguồn nhân lực trong CISA[2]. CISA tập trung vào các hoạt động kiểm toán và quản trị

[1] ISO, "ISO/IEC27001:2005," http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber =42103.
[2] Xem ISACA, "Standards for Information Systems Auditing," http://www.isaca.org/Template.cfm?Section=CISA_Certification&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=16&ContentID=19566.

hệ thống thông tin. Theo đó, vai trò của kiểm toán viên và hiệu quả của quá trình kiểm toán được xem là rất quan trọng.

CISSP[3] thì chủ yếu tập trung và an ninh các yếu tố kỹ thuật. Nó nhấn mạnh công tác sắp xếp và điều hành trang thiết bị như các hệ thống máy tính và máy chủ.

Bài tập

1. Đánh giá mức độ nhận thức về an ninh thông tin của các thành viên trong đơn vị bạn.
2. Các biện pháp an ninh thông tin được thực hiện trong đơn vị của bạn là gì? Phân loại các biện pháp này theo những tiêu chí của 4 phương pháp an ninh thông tin.
3. Cho ví dụ về các biện pháp an ninh thông tin theo các lĩnh vực quản trị điều hành, các yếu tố vật chất và kỹ thuật trong tổ chức của bạn hoặc tại các tổ chức khác trong vùng hay quốc gia bạn sống.

Các thành viên tham dự khóa học có thể làm bài tập theo nhóm. Nếu các thành viên đến từ nhiều quốc gia khác nhau, việc phân nhóm có thể tiến hành theo mỗi quốc gia.

Tự kiểm tra

1. Thông tin khác với các tài sản khác như thế nào?
2. Tại sao an ninh thông tin liên quan tới một chính sách?
3. Các cách thức đảm bảo an ninh thông tin là gi? Phân biệt các phương pháp tiến hành an ninh thông tin.
4. Phân biệt sự khác nhau giữa ba phạm vi an ninh thông tin (quản trị điều hành, các yếu tố vật chất, các yếu tố kỹ thuật).

[3] Xem (ISC)², “CISSP® - Certified Information Systems Security Professional,” http://www.isc2.org/cissp.

2. CÁC ĐỊNH HƯỚNG VÀ XU HƯỚNG AN NINH THÔNG TIN

Phần này nhằm mục đích:

. Giới thiệu các mối đe dọa đối với an ninh thông tin; và

. Miêu tả các biện pháp đối phó chống lại các mối đe dọa này.

2.1. Các kiểu tấn công an ninh thông tin

Thâm nhập trái phép (Hacking)

Hacking là một hành động truy cập tới một máy tính hoặc mạng máy tính nhằm giành được hay chỉnh sửa thông tin mà không có sự cho phép hợp pháp.

Hacking có thể được phân loại thành hình thức thâm nhập mang tính tiêu khiển, tội phạm hay mang tính chính trị, tùy thuộc vào mục đích của cuộc tấn công. Hacking mang tính tiêu khiển là việc thay đổi trái phép các chương trình hay dữ liệu một cách đơn giản nhằm thỏa mãn sự tò mò của tin tặc (hacker). Hacking mang tính chất tội phạm được sử dụng trong hoạt động gian lận và gián điệp. Hacking mang tính chính trị là hình thức can thiệp vào các website để quảng bá những thông điệp chính trị không được phép.[4]

Gần đây, hacking ngày càng gắn liền với khủng bố mạng và chiến tranh mạng, tạo ra một mối đe dọa lớn đối với an ninh quốc gia.

Từ chối dịch vụ (DoS)

Tấn công từ chối dịch vụ ngăn chặn người dùng hợp pháp sử dụng một dịch vụ nào đó trong khi kẻ phạm tội giành quyền truy nhập tới hệ thống máy móc hoặc dữ liệu. Tình huống này xảy ra khi kẻ tấn công "làm tràn" một hệ thống mạng với khối lượng lớn dữ liệu hoặc cố ý chiếm dụng nguồn tài nguyên giới hạn, như việc chặn đứng khả năng kiểm soát tiến trình hay xếp hàng chờ

[4] Suresh Ramasubramanian, Salman Ansari and Fuatai Purcell, "Governing Internet Use: Spam, Cybercrime and e-Commerce," in Danny Butt (ed.), Internet Governance: Asia-Pacific Perspectives (Bangkok: UNDP-APDIP, 2005), 95, http://www.apdip.net/projects/igov/ICT4DSeries-iGov-Ch5.pdf.

các kết nối mạng. Hoặc chúng có thể phá hỏng các thành phần vật lý trong mạng lưới thao túng dữ liệu trong quá trình truyền đưa, kể cả dữ liệu đã được mã hóa.[5]

Chiến tranh mạng giữa Mỹ và Trung Quốc

Một nhóm tin tặc có tên PoizonBox tại Mỹ đã bị buộc tội xóa sổ hơn 350 website của Trung Quốc trong vòng 1 tháng. Nhóm này cũng bị cho là đã tấn công 24 website Trung Quốc, trong đó có website của 8 tổ chức chính phủ Trung Hoa, ngày 30/4/2001. Các tin tặc Trung Quốc sau đó đã tuyên bố Cuộc chiến tranh mạng lần thứ 6 với Bộ Quốc Phòng và đánh vào các website Mỹ từ 30/4 – 1/5/2001, trong đó có website của các tổ chức chính phủ Mỹ. Các cuộc tấn công đã khiến Lầu năm góc phải nâng tình trạng an ninh các hệ thống máy tính của mình từ INFO-CON NORMAL lên INFO-CON ALPHA. Ngày 1/5/2001, Trung tâm Bảo vệ Hạ tầng quốc gia của Cục điều tra Liên Bang đưa ra cảnh báo rằng tin tặc Trung Quốc đã tấn công website của các công ty và chính phủ Mỹ.

Sau cuộc chiến tranh mạng này, Mỹ nhận ra rằng các hiểm họa điện tử (giống như hacking) có thể là nguyên nhân gây ra nhiều thiệt hại cho các tổ chức chính phủ Mỹ và sau đó đã tăng cường khả năng phòng thủ chống lại các mối đe dọa mạng thông qua việc nâng mức ngân sách tài chính cho an ninh thông tin và cải thiện chính sách thông tin bên trong các tổ chức chính phủ.

Nguồn: Attrition.org, "Cyberwar with China: Self-fulfilling Prophecy" (2001), http://attrition.org/security/commentary/cn-us-war.html.

[5] ESCAP, "Module 3: Cyber Crime and Security," http://www.unescap.org/icstd/POLICY/publications/internet-use-for-business-development/module3-sources.asp.

Khủng bố mạng chống lại Estonia

Ngày 4/5/2007 tại thủ phủ của Estonia, cuộc di dời đài tưởng niệm của Liên bang Xô Viết từ trung tâm thành phố tới một nghĩa trang quân đội đã kích động cuộc tấn công khủng bố mạng kéo dài ba tuần chống lại Estonia, trong đó có tấn công từ chối dịch vụ DoS với khoảng 1 triệu máy tính. Website và mạng máy tính của phủ tổng thống, Quốc hội Estonia, nhiều cơ quan chính phủ, đảng cầm quyền, báo chí và ngân hàng bị đánh sập. Thậm chí mạng không dây cũng là mục tiêu của cuộc tấn công.

Sau đó, Estonia đã tìm ra vị trí của kẻ tấn công nằm tại một tổ chức chính phủ của Nga. Chính phủ Nga đã phủ quyết cáo buộc này.

Khi cuộc tấn công khủng bố mạng xảy ra, Estonia không thể đối phó ngay lập tức do thiếu một đội phản ứng nhanh và không có chính sách an ninh thông tin.

Nguồn: Beatrix Toth, "Estonia under cyber attack" (Hun-CERT, 2007), http://www.cert.hu/dmdocuments/Estonia_attack2.pdf.

Mã độc (Malicious code)

Mã độc được hiểu là các chương trình có thể gây ra những hư hại cho một hệ thống khi được thực thi. Virus, sâu worm và Trojan là các loại của mã độc.

Virus máy tính là một chương trình hay mã lập trình gây hư hai cho dữ liệu và hệ thống máy tính bằng cách tự tái tạo thông qua bản sao chép ban đầu tới một chương trình, phân vùng khởi động máy tính hay tài liệu khác.

Sâu máy tính là một loại virus có khả năng tự tái tạo mà không làm biến đổi tệp tin (file) nhưng nó thường trú trong bộ nhớ chính, sử dụng một phần hệ điều hành, vô thức và thường vô hình đối với người dùng. Việc không kiểm soát được sự nhân bản của chúng dân tới tiêu tốn tài nguyên hệ thống, gây chậm hoặc tắc nghẽn các tác vụ khác.

Trojan là một chương trình mà sự xuất hiện của nó là hữu ích và/hoặc vô hại, nhưng thật ra nó có một chức năng nguy hiểm như các chương trình ẩn tự động tải dữ liệu lên hoặc các đoạn mã lệnh khiến cho một hệ thống có thể bị tấn công, xâm phạm.

Cuộc khủng bố Internet 1.25 tại Hàn Quốc

Ngày 25/01/2003, một virus máy tính có tên "Slammer worm" đã gây ra sự cố ngắt các kết nối Internet trên toàn quốc tại Hàn Quốc. Sự cố này rốt cuộc kéo dài hơn 9 giờ đồng hồ, được xác định nguyên nhân là do dịch vụ máy chủ tên miền(DNS) bị đánh sập bởi sâu máy tính.

Hậu quả của sự cố khiến thị trường mua bán trực tuyến bị thiệt hại một khoản ước tính 200.000 – 500.000 USD và tổng giá trị giao dịch trực tuyến bị thất thoát lên tới 22,5 tỉ USD. Kết quả báo cáo cho thấy thiệt hại do Slammer worm gây ra lớn hơn cả thiệt hại gây bởi virus CodeRed và Nimda vì nạn nhân chỉ là những người dùng bình thường.

Cuộc khủng bố Internet đã thúc đẩy chính phủ Hàn Quốc thông qua công tác quản lý toàn diện đối với các nhà cung cấp dịch vụ Internet (ISP) và Công ty an ninh thông tin (Information Security Company). Các hệ thống an ninh thông tin và bảo vệ hạ tầng thông tin đã được thiết lập, và một ban hay đơn vị an ninh thông tin được xây dựng trong mỗi tổ chức.

Kiến trúc xã hội (Social engineering)

Thuật ngữ "kiến trúc xã hội" dùng để chỉ một bộ kỹ thuật được sử dụng để lôi kéo người dùng trong việc bày tỏ, chia sẻ các thông tin mang tính bí mật. Mặc dù nó cũng tương tự như một thủ đoạn hay sự gian lận đơn giản, hình thức điển hình này được áp dụng để để thu thuật thông tin hay truy nhập hệ thống máy tính. Trong hầu hết các trường hợp, kẻ tấn công không bao giờ đối mặt với nạn nhân.

Tấn công lừa đảo (Phishing)

Phishing là hành động lấy cắp thông tin cá nhân thông qua Internet nhằm mục đích lừa gạt tài chính, đây là một ví dụ của Social engineering. Phishing ngày càng trở thành một hoạt động tội phạm quan trọng trên mạng Internet.

Vụ tấn công Ngân hàng Thụy Sĩ được biết đến là vụ ăn cắp trực tuyến "lớn chưa từng có"

Ngày 19/01/2007, ngân hàng Thụy Sĩ Nordea bị tấn công bằng hình thức lừa đảo trực tuyến phishing. Cuộc tấn công bắt đầu từ một Trojan tự tạo được gửi dưới danh nghĩa của ngân hàng tới một số khách hàng. Người gửi khuyến khích khách hàng tải một ứng dụng "ngăn chặn thư rác". Người dùng tải về tệp tin đính kèm có tên ranking.zip hoặc ranking.exe đã bị nhiễm Trojan được biết đến là haxdoor.ki bởi một số công ty bảo mật.

Thực chất haxdoor đã cài đặt trình theo dõi thao tác bàn phím keylogger để ghi lại những thông tin đánh cắp và có khả năng tự ẩn mình nhờ sử dụng công cụ rootkit (*là công cụ phần mềm do kẻ xâm nhập đưa vào máy tính nhằm mục đích cho phép mình quay lại xâm nhập máy tính đó và dùng nó cho các mục đích xấu mà không bị phát hiện*). Các biến kể .ki của Trojan được kích hoạt khi khách hàng đăng nhập vào trang (site) trực tuyến của ngân hàng Nordea. Khách hàng bị chuyển tới một trang chủ giả mạo, nơi họ điền các thông tin đăng nhập quan trọng, kể cả số lần đăng nhập. Sau khi khách hàng điền thông tin, một thông báo lỗi xuất hiện, thông báo với họ rằng site đang gặp phải các sự cố kỹ thuật. Kẻ phạm tội sau đó sử dụng thông tin chi tiết của khách hàng thu được trên website thật của ngân hàng Nordea để rút tiền từ tài khoản khách hàng.

Khách hàng của Nordea bị lừa đảo bằng e-mail có chứa Trojan trong hơn 15 tháng. 250 khách hàng phản ánh bị ảnh hưởng với tổng thiệt hại ước tính khoảng 7 – 8 triệu krona Thụy Sĩ (7.300 – 8.300USD). Tình huống này minh chứng rằng tấn công mạng có thể ảnh hưởng tới cả các công ty tài chính có mức độ bảo mật cao.

Nguồn: Tom Espiner, "Swedish bank hit by 'biggest ever' online heist," ZDNet.co.uk (19 January 2007), http://news.zdnet.co.uk/security/0,1000000189, 39285547,00.htm.

2.2. Xu hướng của các mối hiểm họa an ninh thông tin[6]

Một hoạt động quan trọng trong công tác bảo đảm an ninh thông tin là phân tích xu hướng của hiểm họa an ninh. Điều này hướng tới việc tìm kiếm các mô hình hiểm họa an ninh theo trật tự thời gian để nhận biết cách thức chúng thay đổi và phát triển, xoay theo một chiều hướng mới hay chuyển đổi. Quá trình liên tục thu thập, liên kết thông tin và phát triển các đặc trưng đi kèm này được thực hiện để có thể lường trước các nguy cơ tương tự hoặc có thể đồng thời chuẩn bị những đối sách phù hợp đối phó với những hiểm họa đó.

Những tổ chức thực hiện việc phân tích xu hướng các mối hiểm họa an ninh thông tin và chia sẻ các báo cáo hiểm họa an ninh thông tin gồm có:

- CERT (http://www.cert.org/cert/)
- Symantec (http://www.symantec.com/business/theme.jsp?themeid=threatreport)
- IBM (http://xforce.iss.net/)

Dưới đây là mô tả về các xu hướng hiểm họa an ninh thông tin đã được báo cáo:

Các công cụ tấn công tự động[7]

Ngày nay, những kẻ xâm nhập sử dụng các công cụ tự động cho phép chúng có thể thu thập thông tin của hàng ngàn máy chủ lưu trữ Internet (host) một cách dễ dàng và nhanh chong. Hệ thống mạng có thể bị quét từ một vị trí ở xa và với các host được nhận định là có điểm yếu sẽ sử dụng những công cụ tự động này. Kẻ xâm nhập ghi lại những thông tin cho mục đích sử dụng sau này, chia sẻ hoặc giao dịch với những kẻ xâm nhập khác hoặc có thể tấn công ngay lập tức. Một số công cụ (như Cain&Abel) tự động thực hiện một loạt những tấn công nhỏ nhắm tới một mục tiêu tổng thể. Ví dụ, kẻ xâm nhập có thể sử dụng một chương trình nghe trộm gói tin (packet sniffer) để lấy mật khẩu của router hoặc firewall, đăng nhập vào firewall để vô hiệu hóa bộ lọc (filter), và sau đó sử dụng một dịch vụ tệp tin mạng để đọc dữ liệu trên máy chủ.

---

[6] Được trích từ Tim Shimeall and Phil Williams, *Models of Information Security Trend Analysis* (Pittsburgh: CERT Analysis Center, 2002), http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.11.8034.
[7] Được trích từ CERT, "Security of the Internet," Carnegie Mellon University, http://www.cert.org/encyc_article/tocencyc.html

Các công cụ tấn công khó phát hiện

Một số công cụ tấn công sử dụng mô hình tấn công kiểu mới mà không bị phát hiện bởi các công cụ dò tìm hiện tại. Ví dụ, các kỹ thuật anti – forensic được sử dụng để che dấu hay ẩn đi bản chất của những công cụ tấn công. Các công cụ đa dạng thay đổi hình thức theo mỗi lần chúng được sử dụng. Một vài công cụ này sử dụng các giao thức chung như giao thức truyền tải siêu văn bản (HTTP) khiến cho khó có thể phân biệt chúng với giao dịch mạng hợp pháp.[8] Sâu MSN Messenger là một ví dụ điển hình cho tình huống này. Sâu trong trình nhắn tin nhanh (IM) MSN Messenger gửi tới các danh bạ trong sổ địa chỉ của người bị nhiễm một tệp tin được thiết kế để xâm nhập vào hệ thống sau khi đưa ra cảnh báo lần đầu rằng họ nhận nhận một tệp tin. Các hành động trên trình IM của người sử dụng bị bắt chước, gây ra sự hoang mang.[9]

Khôi phục nhanh hơn các khả năng bị tấn công

Hàng năm, số lượng các sản phẩm phần mềm khôi phục khả năng bị tấn công mới được báo cáo tới Trung tâm đối ứng sự cố máy tính Computer Emergency Response Team Coordination Center (CERT/CC) nhiều hơn gấp đôi, gây khó khăn cho các nhà quản trị trong việc cập nhật các bản vá (patch). Những kẻ xâm nhập biết điều đó và chiếm lợi thế.[10] Một số kẻ xâm nhập tiến hành tấn công zero-day hoặc zero-hour (lỗ hổng chưa được công bố), theo đó một máy tính có nguy cơ bị khai thác qua các ứng dụng có khả năng bị tấn công mà không có bản vá hay sự bảo vệ bởi chúng chưa được phát hiện bởi nhà quản trị.[11]

Sự gia tăng hiểm họa bất đối xứng và sự hội tụ các phương thức tấn công

Hiểm họa bất đối xứng là một tình huống mà trong đó kẻ tấn công có lợi thế vượt trên cả khả năng chống đỡ. Số lượng các mối hiểm hoạ bất đối xứng gia tăng cùng với khả năng tự động hóa của sự phát triển hiểm họa cũng như tính chất tinh vi của các công cụ tấn công.

---

[8] Suresh Ramasubrahmanian et al., op. cit., 94.
[9] Munir Kotadia, "Email worm graduates to IM," ZDNet.co.uk (4 April 2005), http://news.zdnet.co.uk/security/0,1000000189,39193674,00.htm.
[10] Suresh Ramasubrahmanian et al., op. cit.
[11] Wikipedia, "Zero day attack," Wikimedia Foundation Inc., http://en.wikipedia.org/wiki/Zero_day_attack.

Sự hội tụ các phương thức tấn công thể hiện sự thống nhất các cách thức tấn công khác nhau của kẻ thực hiện nhằm tạo ra hệ thống mạng toàn cầu nhằm hỗ trợ cho hoạt động phá hại được sắp xếp. Một ví dụ là Mpack, đây là Trojan được cài đặt lên máy tính của người dùng thông qua việc giao tiếp với các máy chủ Mpack. Kẻ tấn công tạo ra các giao dịch tới những máy chủ này bằng cách phá hại các website chính thức vì thế những khách viếng thăm website này sẽ được chuyển hướng tới máy chủ Web giả mạo, hoặc bằng cách gửi đường liên kết (link) tới máy chủ Web giả mạo thông qua các thông điệp thư rác (spam). Những máy chủ Web giả mạo này sẽ chuyển hướng trình duyệt của người dùng tới các máy chủ Mpack.[12]

Sự gia tăng các nguy cơ tấn công cơ sở hạ tầng

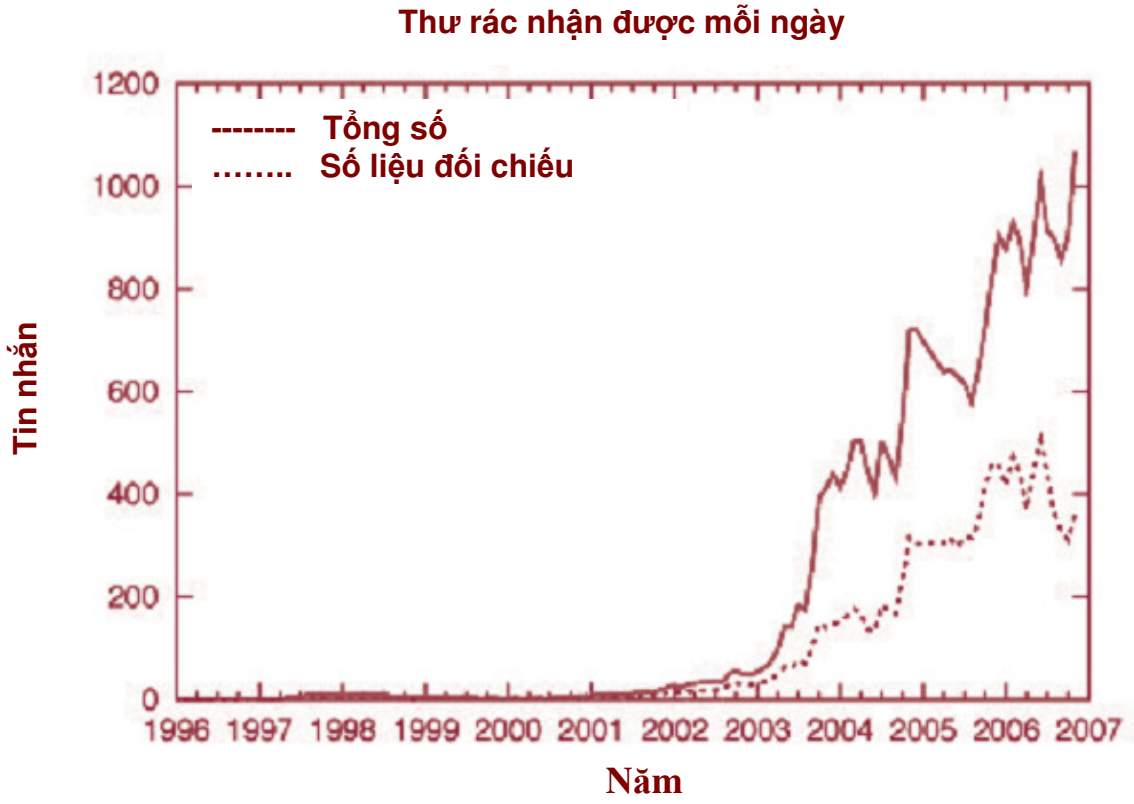
Tấn công cơ sở hạ tầng là những tấn công có ảnh hưởng sâu rộng tới các thành phần chủ chốt của mạng Internet. Chúng là mối quan tâm bởi số lượng các tổ chức và người sử dụng Internet cũng như sự gia tăng tính phụ thuộc đối với Internet của họ trong việc thực hiện các hoạt đông kinh doanh hàng ngày. Hậu quả của các cuộc tấn công cơ sở hạ tầng với hình thức DoS, làm thiệt hại các thông tin nhạy cảm, phát tán tin tức sai và làm chệch đi đáng kể các nguồn lực từ những nhiệm vụ khác.

Botnet là một ví dụ về tấn công cơ sở hạ tầng. Thuật ngữ botnet dùng để chỉ một nhóm các máy tính nhiễm độc bị điều khiển từ xa bởi một máy chủ điều lệnh (command control server). Các máy tính bị nhiễm độc sẽ phát tán sâu và Trojan thông qua hệ thống mạng.

Thư rác nhanh chóng tăng lên do sử dụng botnet. Thư rác là những thông điệp không mong muốn có số lượng lớn có thể được gửi thông qua e-mail, tin nhắn, các động cơ tìm kiếm, blog và thậm chí là qua điện thoại di động. Hình 4 cho thấy xu hướng gia tăng lượng thư rác.

[12] Symantec, Symantec Internet Security Threat Report: Trends for January–June 07, Volume XII (September 2007), 13, http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_exec_summary_09_2007.en-us.pdf.

Hình 4. Hiện trạng thư rác



Đối phó với Botnet

Để giảm thiệt hại do botnet gây ra, Liên minh viễn thông quốc tế (ITU) khuyến nghị một sự kết hợp giữa chính sách, công nghệ và phương pháp luận mang tính xã hội.

Về chính sách: Các quy tắc và luật tội phạm mạng, chống thư rác có hiệu quả

- Xây dựng năng lực giữa các đối tượng nắm giữ chính sách có liên quan
- Khuôn khổ toàn diện cho các hoạt động và hợp tác quốc tế
- Nhất quán giữa pháp chế về tội phạm mạng và sự riêng tư
- Khuôn khổ cho việc thi hành tại đơn vị về giảm thiểu tội phạm mạng và botnet

Về kỹ thuật: Các kỹ thuật và công cụ nhận diện cũng như thu thập thông tin về những botnet thực sự

- Những bài thực hành tốt nhất cho ISP để giảm thiểu các hoạt động botnet
- Những bài thực hành tốt nhất cho cán bộ đào tạo và cơ quan đăng ký để giảm thiểu các hoạt động botnet
- Xây dựng năng lực cho các nhà cung cấp giao dịch trực tuyến và thương mại điện tử

Về xã hội: Sáng kiến đào tạo rộng rãi về an ninh và an toàn Internet

- Tạo điều kiện thuận lợi về các truy nhập ICT bảo đảm cho người dùng

Bộ công cụ PTF ITU SPAM là một gói giải pháp toàn diện giúp các nhà hoạch định chính sách, nhà quản lý và các doanh nghiệp trong việc điều chỉnh chính sách và khôi phục tính riêng tư đối với e-mail. Bộ công cụ này cũng khuyến nghị việc chia sẻ thông tin giữa các quốc gia nhằm ngăn chặn những sự cố mang tầm quốc tế.

Thay đổi mục đích tấn công

Trước đây, các cuộc tấn công mạng và máy tính thường xảy ra vì tính hiếu kỳ hay tự thỏa mãn bản thân. Ngày nay, mục đích tấn công thường là vì tiền bạc, vu khống và phá hoại. Hơn nữa, những kiểu tấn công này chỉ thể hiện cho một phần nhỏ trong phạm vi rộng lớn của tội phạm mạng.

Tội phạm mạng là hình thức phá hoại có chủ ý, đánh sập hay làm sai lệch dữ liệu số hoặc các luồng thông tin vì các nguyên nhân chính trị, kinh tế, tôn giáo hay hệ tư tưởng. Hầu hết các hình thức tội phạm phổ biến bao gồm xâm nhập trái phép, từ chối dịch vụ, mã độc và kiến trúc xã hội. Gần đây, tội phạm mạng đã trở thành một phần của khủng bố mạng và chiến tranh mạng với các tác hại tới an ninh quốc gia.

Bảng 3 dưới đây cho thấy những gì mà thủ phạm của tội phạm mạng kiếm được.

Bảng 3. Thống kê từ tội phạm mạng năm 2007

Tài sản	Định giá (bằng USD)
Chi trả cho mỗi lần cài đặt quảng cáo duy nhất	30 cents tại Mỹ, 20 cents tại Canada, 10 cents tại Anh, 2 cents tại những nơi khác
Gói phần mềm gây hại (Malware), phiên bản cơ bản	1.000USD – 2.000USD
Gói phần mềm gây hại (Malware) với dịch vụ đi kèm	Giá cả không cố định với mức khởi đầu 20USD
Cho thuê bộ thủ thuật phá hoại (Exploit kit) trong 1 giờ	0,99USD – 1USD
Cho thuê bộ thủ thuật phá hoại (Exploit kit) trong 2,5 giời	1,60USD – 2USD
Cho thuê bộ thủ thuật phá hoại (Exploit kit) trong 5 giờ	4USD, có thể nhiều hơn
Trojan đánh cắp thông tin mà không bị	80USD, có thể nhiều hơn

phát hiện	
Tấn công DoS phân tán	100USD/ngày
10.000 máy tính bị nhiễm độc	1.000USD
Đánh cắp tài khoản tín dụng ngân hàng	Giá cả không cố định với mức khởi đầu 50USD
1 triệu địa chỉ e-mail mới thu thập được (không kiểm định)	8USD trở lên, phụ thuộc vào chất lượng

Nguồn: Trend Micro, 2007 Threat Report and Forecast (2007), 41, http://trendmicro.mediaroom.com/file.php/66/2007+Trend+Micro+Report_FINAL.pdf

2.3. Cải thiện an ninh, bảo mật

Do xu hướng về các mối đe dọa an ninh và các công nghệ tấn công, phòng thủ mạnh mẽ đòi hỏi một chiến lược linh hoạt, cho phép thích ứng với môi trường thay đổi, các thủ tục và chính sách rõ ràng, việc sử dụng các công nghệ bảo mật thích hợp, và cảnh giác không ngừng.

Một điều hữu ích đó là bắt đầu chương trình cải tiến bảo mật bằng việc xác định hiện trạng an ninh. Không thể thiếu đối với một chương trình bảo mật là các tài liệu về chính sách và thủ tục, cũng như công nghệ hỗ trợ cho việc thực hiện.

Quản trị an ninh

Quản trị an ninh bao gồm một chiến lược an ninh thông tin, chính sách và các đường lối chỉ đạo.

Một **chiến lược an ninh thông tin** đặt ra định hướng cho tất cả các hoạt động an ninh thông tin.

Một **chính sách an ninh thông tin** là một tài liệu kế hoạch ở mức cao cho an ninh thông tin của toàn bộ tổ chức. Nó cung cấp một khuôn khổ cho việc ra các quyết định, như một kế hoạch an ninh vật lý và quản trị.

Bởi một chính sách an ninh thông tin có quan điểm dài hạn, nó nên tránh đề cập đến một công nghệ nhất định, và bao hàm sự phát triển kế hoạch hoạt động liên tục hiệu quả.

Đường lối chỉ đạo an ninh thông tin được xây dựng dựa trên chính sách và chiến lược an ninh thông tin. Đường lối chỉ đạo sẽ chỉ rõ các quy tắc cho mỗi lĩnh vực liên quan đến an ninh thông tin. Và do đường lối chỉ đạo phải bao hàm toàn diện trên phạm vi quốc gia, chúng phải được phát triển và đưa ra bởi chính phủ, được thực hiện bởi các tổ chức.

Các tiêu chuẩn an ninh thông tin phải được chuyên biệt hóa và cụ thể do đó chúng có thể được áp dụng cho tất cả các lĩnh vực an ninh thông tin. Một điều thuận lợi cho mỗi quốc gia để phát triển các tiêu chuẩn sau khi phân tích các tiêu chuẩn an ninh kỹ thuật, vật lý và quản trị thì chúng được sử dụng rộng rãi trên toàn thế giới. Các tiêu chuẩn sẽ được dành riêng cho môi trường ICT đang phổ biến.

Chiến lược, chính sách và đường lối chỉ đạo an ninh thông tin của một quốc gia sẽ tuân thủ quy tắc có liên quan. Phạm vi của chúng sẽ nằm cho ranh giới của các luật lệ quốc tế và quốc gia.

Tiến trình và sự vận hành an ninh thông tin

Một khi các đường lối, chính sách và chiến lược an ninh thông tin được xây dựng, các tiến trình và thủ tục vận hành an ninh thông tin cũng sẽ cần được xác định. Bởi kẻ phạm tội tấn công vào thông tin hay kẽ hở thông tin nội bộ, do đó quản lý nguồn nhân lực là yếu tố quan trọng nhất trong vận hành an ninh thông tin. Do đó cần chú ý những vấn đề sau đây:

1. Chương trình giáo dục và đào tạo về an ninh thông tin – Có nhiều phương pháp để cải thiện mức độ an ninh thông tin của một tổ chức tuy nhiên giáo dục và đào tạo là những hoạt động cơ bản. Các thành viên của một tổ chức phải đánh giá đúng nhu cầu đối với an ninh thông tin và đạt được các kỹ năng liên quan thông qua quá trình đào tạo. Tuy nhiên, điều quan trọng là phát triển nhiều các chương trình để tối đa hóa sự tham gia bởi vì các chương trình giáo dục, đào tạo về an ninh thông tin được tiêu chuẩn hóa có thể không hiệu quả.

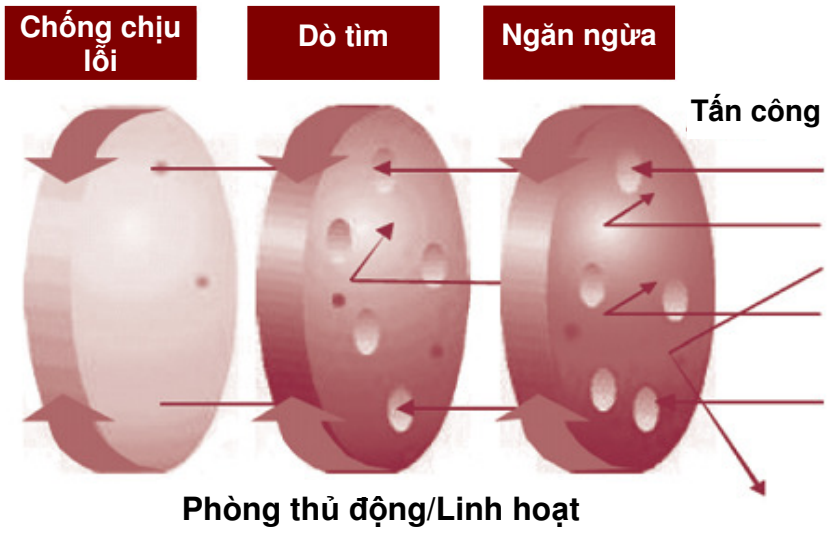
2. Tăng cường các hoạt động xúc tiến thông qua rất nhiều sự kiện – Sự tham gia của người lao động có vai trò quan trọng đối với việc thực hiện thành công đường lối chỉ đạo, chính sách và chiến lược an ninh thông tin. An ninh thông tin sẽ được đẩy mạnh trong đội ngũ người lao động thông qua các hoạt động hàng ngày.
3. Bảo đảm trách nhiệm của người đứng đầu – Trong khi người lao động có thể có nhận thức cao về an ninh thông tin và họ có quyết tâm lớn để duy trì an ninh thông tin thì rất khó để đảm bảo an ninh thông tin mà không có sự hỗ trợ từ cấp lãnh đạo cao nhất trong tổ chức. Cần phải có được sự ủng hộ từ Chủ tịch Hội đồng quản trị (Chief Executive Officer) và Giám đốc Công nghệ thông tin (Chief Information Officer).

An ninh về mặt công nghệ

Có rất nhiều công nghệ đã được phát triển để giúp các tổ chức bảo đảm cho hệ thống thông tin của mình chống lại những kẻ xâm nhập. Những công nghệ này giúp cho thông tin và các hệ thống có thể chống lại các cuộc tấn công, dò tìm các hoạt động nghi ngờ và bất thường, đồng thời đối phó những vấn đề phát sinh được coi là an ninh hiệu quả.

Các hệ thống an ninh ngày nay được thiết kế và phát triển dựa trên mô hình *Phòng thủ theo chiều sâu* DID (Defense In Depth) dẫn tới việc quản lý đồng bộ những công nghệ liên quan. Mô hình này khác với mô hình phòng thủ vành đai, chỉ có một lớp phòng thủ chống lại các hiểm họa. Mô hình DID bao gồm việc ngăn ngừa, dò tìm và chống chịu lỗi, với các mối hiểm họa được giảm bớt theo mỗi pha (Hình 5).

Hình 5. Mô hình phòng thủ theo chiều sâu DID



Nguồn: Defense Science Board, Protecting the Homeland: Defensive Information Operations 2000 Summer Study Volume II (Washington, D.C.: Defense Science Board, 2001), 5, http://www.acq.osd.mil/dsb/reports/dio.pdf

Công nghệ ngăn ngừa (Prevention Technology)

Các công nghệ ngăn ngừa bảo vệ chống lại những kẻ tấn công và các mối hiểm họa về lưu trữ hay ở cấp độ hệ thống. Những công nghệ này bao gồm:

1. Mật mã (Cryptography): Cũng được xem là mã hóa, mật mã là một quá trình dịch thông tin từ định dạng gốc (dưới hình thức văn bản – plaintext) thành định dạng được mã hóa, khó hiểu (được gọi là văn bản mật mã – ciphertext). Giải mã được hiểu là quá trình tác động vào ciphertext và dịch ngược nó trở lại thành plaintext. Mật mã được sử dụng để bảo vệ rất nhiều ứng dụng. Thông tin về mật mã và các công nghệ liên quan (IPSec, SSH, SSL, VPN, OTP, …) có thể tìm thấy nhiều hơn tại các trang web sau:
   - IETF RFC (http://www.ietf.org/rfc.html)
   - RSA Laboratories' Frequently Asked Questions About Today's Cryptography (http:// www.rsa.com/rsalabs/node.asp?id=2152)
2. Mật khẩu sử dụng 1 lần (One-time passwords - OTP): Như tên gọi, OPT chỉ có thể sử dụng được một lần. Mật khẩu tĩnh có thể dễ bị truy nhập hơn thông qua các kỹ thuật đánh cắp mật khẩu (password loss), đánh hơi mật khẩu (password sniffing), bẻ khóa mật khẩu bằng thuật toán "vét cạn" (brute-force password cracks) và các hình thức tương tự. Hiểm họa này có thể được giảm đi rất nhiều nhờ việc thay đổi mật khẩu một cách liên tục,

như được thực hiện với OTP. Vì lý do này, OTP được sử dụng để đảm bảo cho các giao dịch tài chính điện tử như dịch vụ ngân hàng trực tuyến (online banking).

3. Tường lửa (Firewalls): Tường lửa quản lý một số luồng giao dịch giữa các mạng máy tính có các mức độ tin cậy khác nhau như giữa mạng Internet – khu vực không có độ tin cậy, và một mạng nội bộ – khu vực có độ tin cậy cao hơn. Một khu vực với mức độ tin cậy trung bình, được đặt ở vị trí giữa mạng Internet và một mạng nội bộ tin cậy thì thường được hiểu như một "mạng vành đai" (perimeter network) hay vùng phi quân sự (demilitarized zone).
4. Công cụ phân tích khả năng bị tấng công (Vulnerability analysis tool): Do sự gia tăng về số lượng các phương thức tấn công cũng như khả năng bị tấn công trong những ứng dụng thông thường, cần đánh giá thường xuyên về khả năng bị tấn công của hệ thống. Trong an ninh máy tính, một khả năng bị tấn công là một điểm yếu cho phép kẻ tấn công xâm phạm hệ thống. Các khả năng bị tấn công có thể là kết quả từ những mật khẩu yếu, lỗi phần mềm, virus máy tính, một đoạn mã nhiễm độc, chèn lệnh SQL (SQL Injection) hay phần mềm độc hại. Các công cụ phân tích khả năng bị tấn công cung cấp các dịch vụ phân tích. Tuy nhiên, những công cụ này cung cấp miễn phí bởi cộng đồng Internet có thể bị lợi dụng bởi kẻ xâm nhập. Để biết thêm thông tin, có thể xem tại:
   - INSECURE Security Tool (http://sectools.org)
   - FrSIRT Vulnerability Archive (http://www.frsirt.com/english)
   - Secunia Vulnerability Archive (http://secunia.com)
   - SecurityFocus Vulnerability Archive (http://www.securityfocus.com/bid)

Các công cụ phân tích khả năng tấn công mạng lưới có thể sử dụng để phân tích khả năng tấn công các nguồn tài nguyên mạng như bộ định tuyến (router), tường lửa (firewall) và máy chủ (server).

Một công cụ phân tích khả năng bị tấn công máy chủ sẽ phân tích những khả năng như mật khẩu yếu, cách thức cấu hình yếu và lỗi thiết lập quyền cho phép đối với tệp tin trong hệ thống nội bộ. Công cụ phân tích khả năng bị tấn công máy chủ về tương đối cho chúng ta nhiều kết quả chính xác hơn công cụ phân tích khả năng bị tấn công mạng lưới bởi vì công cụ này phân tích nhiều nguy cơ bị tấn công hơn trong hệ thống nội bộ.

Công cụ phân tích khả năng bị tấn công Web sẽ phân tích những khả năng tấn công của các dịch vụ Web như XSS và SQL Injection. Để biết thêm thông tin, có thể xem tài liệu Open Web Application Security Project tại địa chỉ: http://www.owasp.org/index.php/Top_10_2007.

Công nghệ dò tìm (Detection Technology)

Công nghệ dò tìm được sử dụng để phát hiện và lần theo sự xâm nhập và những trạng thái không bình thường trong mạng lưới hay trong các hệ thống quan trọng. Công nghệ dò tìm bao gồm:

Phần mềm chống virus (Antivirus): Phần mềm chống virus là một chương trình máy tính dùng để nhận diện, loại trừ hay làm vô hiệu mã độc, bao gồm sâu máy tính (worm), tấn công lừa đảo (phishing), rootkit, Trojan và phần mềm độc hại khác (malware).[13]

Hệ thống dò tìm xâm nhập (Intrusion detection system - IDS): Một hệ thống IDS sẽ thu thập và phân tích thông tin từ rất nhiều khu vực trong một máy tính hay một mạng lưới để nhận diện các lỗ hổng an ninh có thể xảy ra. Chức năng dò tìm xâm nhập bao gồm phân tích những mô hình hoạt động bất thường và khả năng phát hiện ra các mô hình tấn công.

Hệ thống ngăn ngừa xâm nhập (Intrusion prevention system - IPS): Việc ngăn ngừa xâm nhập là cố gắng phát hiện ra những đe dọa tiềm năng và đối phó lại với chúng trước khi bị sử dụng trong các cuộc tấn công. Một hệ thống IPS sẽ giám sát lưu lượng mạng lưới và đưa ra các hoạt động ngay lập tức chống lại các mối đe dọa tiềm năng theo một tập các quy tắc được thiết lập bởi nhà quản trị mạng. Ví dụ, hệ thống IPS có thể khóa lưu lượng từ một địa chỉ IP nghi ngờ.[14]

Công nghệ tích hợp (Integration Technology)

Công nghệ tích hợp thực hiện việc tích hợp những chức năng quan trọng đối với an ninh thông tin của các tài sản cốt lõi như dự đoán, dò tìm và lần theo dấu vết xâm nhập. Công nghệ tích hợp bao gồm:

1. Quản trị an ninh tổ chức (Enterprise security management - ESM): Một hệ thống ESM thực hiện quản lý, kiểm soát và điều hành giải pháp an ninh thông tin như một hệ thống IDS và IPS dựa trên một chính sách nhất quán. Nó được sử dụng để tạo ra các giải pháp khác cho những điểm yếu bằng cách sử dụng những lợi thế của mỗi giải pháp an ninh thông tin và tối đa hóa hiệu quả an ninh thông tin theo một chính sách nhất quán.

   Gần đây, các hệ thống ESM có thể quản lý những công nghệ an ninh hiện có một cách tổng hợp do sự thiếu hụt nguồn nhân lực vận hành các công nghệ an ninh, sự gia tăng các cuộc tấn công ở cấp cao hơn như sự hội tụ các phương thức tấn công, và sự nổi lên của các công cụ tấn công khó có thể phát hiện. Với ESM, hiệu quả của công tác quản lý được nâng lên và các biện pháp đối phó chủ động cũng được thiết lập.

[13] Wikipedia, "Antivirus software," Wikimedia Foundation, Inc., http://en.wikipedia.org/wiki/Antivirus_software.
[14] SearchSecurity.com, "Intrusion prevention," TechTarget, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1032147,00.html.

2. Quản trị rủi ro tổ chức (Enterprise risk management - ERM): ERM là một hệ thống giúp dự báo tất cả những rủi ro liên quan tới tổ chức, bao gồm các phạm vi bên ngoài của an ninh thông tin và các biện pháp cấu hình một cách tự động. Việc sử dụng ERM để bảo vệ thông tin đòi hỏi phải xác định được những mục tiêu chính xác về thiết kế và quản lý rủi ro cho sự phát triển của hệ thống. Hầu hết các tổ chức xây dựng và tối ưu các hệ thống ERM của mình thông qua các đơn vị tư vấn an ninh thông tin chuyên nghiệp thay vì tự mình thực hiện công việc đó.

Câu hỏi suy nghĩ

1. Các mối hiểm họa an ninh thông tin trong tổ chức của bạn có khả năng bị tấn công là gì? Tại sao?
2. Những giải pháp công nghệ an ninh thông tin nào được thực hiện trong tổ chức của bạn?
3. Tổ chức của bạn có một chính sách, chiến lược và đường lối chỉ đạo an ninh thông tin hay không? Nếu có, làm thế nào để những yếu tố đó tương xứng với các mối đe dọa mà tổ chức của bạn có khả năng bị tấn công? Nếu không, bằng cách nào bạn khuyến nghị về chính sách, chiến lược và đường lối chỉ đạo an ninh thông tin đối với tổ chức của bạn?

Tự kiểm tra

1. Tại sao việc thực hiện phân tích xu hướng mối đe dọa an ninh thông tin lại quan trọng?
2. Tại sao quản trị nguồn nhân lực lại là yếu tố quan trọng nhất trong các hoạt động an ninh thông tin? Những hoạt động chủ chốt trong quản trị nguồn nhân lực đối với an ninh thông tin là gì?
3. Hãy giải thích mô hình phòng thủ theo chiều sâu Defense-in-Depth của an ninh công nghệ. Nó hoạt động như thế nào?

3. CÁC HOẠT ĐỘNG AN NINH THÔNG TIN

Phần này nhằm mục đích:

- **Đưa ra ví dụ về các hoạt động an ninh thông tin của nhiều quốc gia nhằm cung cấp như một hướng dẫn trong việc tạo lập chính sách an ninh thông tin; và**
- **Làm nổi bật vai trò hợp tác quốc tế trong việc triển khai chính sách an ninh thông tin**

3.1. Các hoạt động an ninh thông tin quốc gia

Chiến lược an ninh thông tin của Mỹ

Sau cuộc tấn công khủng bố ngày 11/9/2001, chính phủ Mỹ đã thành lập Bộ Nội an Hoa Kỳ (Department of Homeland Security) nhằm tăng cường an ninh quốc gia không chỉ chống lại các hiểm họa vật lý mà còn đối phó với những mối đe dọa mạng lưới. Mỹ thực hiện các hoạt động an ninh thông tin mang tính toàn diện và hiệu quả thông qua hệ thống các nhân viên an ninh thông tin (Information Security Officer). Chiến lược an ninh thông tin của Mỹ bao gồm Chiến lược quốc gia cho Bộ Nội an (National Strategy for Homeland Security), Chiến lược quốc gia về An ninh vật lý đối với những tài sản chủ chốt và cơ sở hạ tầng tới hạn (National Strategy for the Physical Security of Critical Infrastructures and Key Assets), và Chiến lược quốc gia về Không gian mạng an toàn (National Strategy to Secure Cyberspace).

Chiến lược quốc gia về Không gian mạng an toàn[15] đặt ra tầm nhìn về an ninh mạng lưới và bảo vệ các tài sản cũng và cở sở hạ tầng tới hạn. Nó xác định các hoạt động và mục tiêu rõ ràng để ngăn chặn những cuộc tấn công mạng lưới nhằm vào các tài sản và cơ sở hạ tầng tới hạn. Năm vấn đề ưu tiên được xác định trong Chiến lược Không gian mạng an toàn đó là:

- Hệ thống Phản ứng an ninh không gian mạng quốc gia (National Cyberspace Security Response System)
- Chương trình giảm thiểu khả năng bị tấn công và đe dọa đối với an ninh không gian mạng quốc gia (National Cyberspace Security Threat and Vulnerability Reduction Program)

[15] The White House, The National Strategy to Secure Cyberspace (Washington, D.C.: The White House, 2003), http://www.whitehouse.gov/pcipb.

- Chương trình đào tạo và trang bị nhận thức về an ninh không gian mạng quốc gia (National Cyberspace Security Awareness and Training Program)
- An ninh không gian mạng các cơ quan chính phủ (Securing Government's Cyberspace)
- Phối hợp an ninh không gian mạng quốc tế và an ninh quốc gia (National Security and International Cyberspace Security Cooperation)

Siết chặt Luật An ninh thông tin (Information Security Law)

Đạo luật tăng cường An ninh mạng năm 2002[16] (Cyber Security Enhancement Act of 2002 - CSEA) bao gồm chương 2 của Luật An ninh quốc nội (Homeland Security Law). Nó đưa ra sự bổ sung về hình phạt đối với loại hình tội phạm mạng, ngoại lệ của việc công bố tình trạng khẩn cấp, những trường hợp mang tính thiện chí, ngăn cấm quảng cáo trên Internet bất hợp pháp, bảo vệ bí mật riêng tư và những vấn đề khác.

Ngoại lệ của việc công bố tình trạng khẩn cấp (Emergency Disclosure Exception - EDE): Trước ngày 11/9, Đạo luật về sự riêng tư trong liên lạc điện tử (Electronic Communications Privacy Act - ECPA) cấm các nhà cung cấp dịch vụ truyền thông điện tử (như các ISP) công bố các liên lạc của người dùng (như thư thoại, e-mail và các tệp tin đính kèm). Quy định EDE cho phép các ISP chia sẻ nội dung của một e-mail hay một liên lạc điện tử với các cơ quan thi hành luật pháp mà không cần đảm bảo tuân theo Đạo luật Ái quốc Mỹ (USA Patriot Act) được ban hành sau ngày 11/9/2001. Các quy định ngoại lệ về tính chất công khai trong trường hợp khẩn cấp đã được củng cố trong luật CSEA. Các cơ quan chính phủ nhận nội dung nghi ngờ được yêu cầu báo cáo tới Bộ trưởng Tư pháp (Attorney General) về ngày công khai, các bên liên quan, số nguyên cáo có liên quan cũng như số lượng liên lạc, trong vòng 90 ngày sau khi công bố.

Ngoại lệ đối với các trường hợp mang tính thiện chí (Good Faith Exception): Luật CSEA quy định miễn trừ phạm tội và trách nhiệm công dân trong trường hợp việc lấy thông tin (eavesdropping) được yêu cầu bởi người chủ hay người điều hành máy tính.

Cấm quảng cáo trên Internet đối với các thiết bị không được phép: ECPA cấm việc sản xuất, phân phối, chiếm giữ và quảng cáo trực tuyến qua đôi dây, miệng và các thiết bị chặn liên lạc điện tử. Các thiết bị lấy thông tin hợp pháp (eavesdropping devices) có thể được quảng cáo. Tuy nhiên, người quảng cáo được yêu cầu để biết các nội dung quảng cáo.

[16] Computer Crime and Intellectual Property Section, SEC. 225. Cyber Security Enhancement Act of 2002 (Washington, D.C.: Department of Justice, 2002), http://www.usdoj.gov/criminal/cybercrime/homeland_CSEA.htm.

Tăng sự trừng phạt đối với các phạm tội máy tính: Theo Đạo luật về Lạm dụng và gian lận máy tính (US Computer Fraud and Abuse Act) việc cố ý truy cập vào một máy tính và gây thiệt hại cho nó mà không có sự cho phép thì được coi là bất hợp pháp. Trước ngày 11/9, bất kỳ cá nhân nào bị phát hiện là phạm tội này đều sẽ bị kết án bỏ tù với mức không hơn 5 năm trong trường hợp lần đầu phạm tội và không hơn 10 năm trong trường hợp phạm tội lần hai. Sau ngày 11/9, sự trừng phạt đối với tội này đã được sửa lại thành bỏ tù không hơn 10 năm trong trường hợp phạm tội lần đầu và không hơn 20 năm đối với trường hợp phạm tội lần hai. Các điều khoản phụ trong CSEA quy định rằng một người phạm tội có thể bị kết án tù không nhiều hơn 20 năm nếu người phạm tội gây ra hoặc cố gắng gây ra tổn hại về thể xác nghiêm trọng; cô ta/anh ta có thể bị kết án chung thân nếu gây ra hoặc cố gắng gây ra cái chết.

Sự miễn trừ trách nhiệm của những người hỗ trợ: ECPA miễn trừ trách nhiệm phạm tội đối với nhà cung cấp dịch vụ thông tin liên lạc hỗ trợ trong việc chặn liên lạc hoặc cung cấp thông tin cho các cơ quan thực thi pháp luật.

Đạo luật Quản lý an ninh thông tin Liên bang (Federal Information Security Management Act - FISMA)[17]: bao gồm chương 3 của Luật chính phủ điện tử (e-Government Act) năm 2002. Luật này bảo vệ mạng lưới hạ tầng quốc gia, và kêu gọi tăng cường nỗ lực bảo vệ an ninh thông tin cho tất cả các công dân, các cơ quan an ninh quốc gia và cơ quan thực thi pháp luật. Các mục tiêu chính của Quản lý An ninh thông tin Liên bang đó là: (1) cung cấp một khuôn khổ toàn diện cho việc tăng cường hiệu quả kiểm soát an ninh thông tin đối với các tài sản và hoạt động; và (2) phát triển các kế hoạch kiểm soát và duy trì đối với công tác bảo vệ thông tin/các hệ thống thông tin, đồng thời cung cấp một cơ chế tăng cường quản lý các chương trình an ninh thông tin.

Chiến lược an ninh thông tin của Liên minh Châu Âu

Trong một thông báo đưa ra vào tháng 5 năm 2006[18], Ủy ban Châu Âu mô tả chiến lược mới của Liên minh Châu Âu (EU) về an ninh thông tin, bao gồm một số biện pháp phụ thuộc lẫn nhau dính dáng đến nhiều bên liên quan. Những biện pháp này gồm có việc thiết lập một Khuôn khổ điều tiết cho các giao tiếp điện tử (Regulatory Framework for Electronic Communications) năm 2002, kết nối với sáng kiến i2010 về việc tạo dựng một Xã hội thông tin Châu Âu (European Information Society), và thành lập Cơ quan An ninh Thông tin và Mạng lưới Châu Âu (European Network and Information Security Agency - ENISA) năm 2004. Theo thông báo, những biện pháp này phản ánh một cách tiếp cận theo 3 khía cạnh của vấn đề an ninh trong Xã hội Thông tin bao gồm

[17] Office of Management and Budget, Federal Information Security Management Act: 2004 Report to Congress (Washington, D.C.: Executive Office of the President of the United States, 2005), http://www.whitehouse.gov/omb/inforeg/2004_fisma_report.pdf.

[18] Europa, "Strategy for a secure information society (2006 communication)," European Commission, http://europa.eu/scadplus/leg/en/lvb/l24153a.htm.

các biện pháp an ninh thông tin và mạng lưới (network and information security - NIS) rõ ràng, khuôn khổ điều tiết đối với các giao tiếp điện tử (bao gồm các vấn đề bảo mật dữ liệu và sự riêng tư), và đấu tranh chống tội phạm mạng.

Thông báo lưu ý những cuộc tấn công nhằm vào các hệ thống thông tin, sự gia tăng của các thiết bị di động, việc hướng tới môi trường điện tử "ambient intelligence" (một môi trường nhạy cảm và phản ứng với sự hiện diện của con người), và nâng cao mức độ nhận thức của người dùng về các vấn đề an ninh chủ đạo mà Ủy ban Châu Âu hướng tới để xác định thông qua đối thoại, hợp tác và trao quyền. Những chiến lược này được mô tả trong thông báo sau:

Đối thoại

. Ủy ban đã đề xuất một loạt các biện pháp được thiết kế để tổ chức một cuộc đối thoại mở, bao gồm và đa dạng những đối tượng liên quan:

. Một phép đo kiểm (chấm điểm) đối với các chính sách quốc gia liên quan đến an ninh thông tin và mạng lưới, nhằm giúp nhận định những thực tiễn có hiệu quả nhất theo đó chúng có thể được triển khai trên một nền tảng rộng lớn trên toàn Châu Âu. Đặc biệt, phép đo này sẽ xác định những hoạt động tối ưu để nâng cao nhận thức của các doanh nghiệp vừa và nhỏ (SME) cũng như người dân về những hiểm họa và thách thức gắn với an ninh thông tin và mạng lưới; và

. Một cấu trúc đa đối tượng liên quan (multi-stakeholder) cân nhắc xem làm thế nào để khai thác tốt nhất những công cụ điều tiết hiện có. Tranh luận này sẽ được tổ chức trong nội dung của các buổi hội thảo, hội nghị.

Hợp tác

. Việc lập chính sách hiệu quả cần có một khả năng nắm bắt rõ ràng về bản chất của các thách thức được chỉ ra, cũng như tính tin cậy, cập nhật của các dữ liệu kinh tế và thống kê.. Theo đó, Ủy ban sẽ yêu cầu ENISA:

. Xây dựng một quan hệ hợp tác tin cậy với các Thành viên Chính phủ và những đối tượng liên quan nhằm phát triển một khuôn khổ thích hợp cho việc thu thập dữ liệu; và

. Kiểm tra tính khả thi về một hệ thống cảnh báo và chia sẻ thông tin Châu Âu nhằm đối phó hiệu quả đối với các mối đe dọa. Hệ thống này là một cổng thông tin Châu Âu đa ngôn ngữ, cung cấp thông tin theo yêu cầu vè các mối hiểm họa, rủi ro và những cảnh báo.

Song song với đó, Ủy ban sẽ mời các Thành viên Chính phủ, khu vực tư nhân và cộng đồng nghiên cứu để tạo nên sự hợp tác nhằm đảm bảo tính sẵn sàng của dữ liệu liên quan đến lĩnh vực an ninh ICT.

Sự trao quyền

Sự trao quyền đối cho những đối tượng liên quan là một điều kiện tiên quyết để kích thích nhận thức của họ về những hiểm họa và nhu cầu an ninh. Vì lý do này, các Thành viên Chính phủ được mời để:

- Tham gia tích cực trong việc đề xuất các phép đo kiểm, chấm điểm điểm những chính sách quốc gia;
- Đẩy mạnh, trong khuôn khổ hợp tác với ENISA, các chiến dịch nhận thức về lợi ích đạt được của các hoạt động, hành vi và những công nghệ an ninh hiệu quả;
- Là đòn bẩy để đưa ra những dịch vụ chính phủ điện tử nhằm thúc đẩy các hoạt động an ninh tích cực; và
- Khuyến khích sự phát triển của các chương trình an ninh thông tin và mạng lưới như một phần của giáo trình giáo dục đại học.

Những đối tượng liên quan trong khu vực tư nhân cũng được khuyến khích nhằm tạo ra các sáng kiến để:

- Xác định trách nhiệm của các ISP và đơn vị sản xuất phần mềm trong quan hệ cung cấp các mức độ an ninh tương xứng và có thể kiểm tra;
- Tăng cường tính đa dạng, tính mở, tính tương hợp, tính hữu dụng và sự cạnh tranh như các nhân tố chính của an ninh, đồng thời khuyến khích sự phát triển của các dịch vụ và sản phẩm bảo mật nâng cao nhằm chống lại hành vi đánh cắp ID và các tấn công xâm nhập – bí mật riêng tư khác;
- Phổ biến các hoạt động an ninh có kết quả tốt cho những nhà điều hành mạng lưới, nhà cung cấp dịch vụ và SME;
- Đẩy mạnh các chương trình đào tạo trong khu vực tư nhân nhằm cung cấp cho nhân viên các kiến thức và kĩ năng cần thiết cho việc thực hiện các hoạt động an ninh;
- Hướng tới các chương trình chứng nhận an ninh cho những dịch vụ, quy trình và sản phẩm mà sẽ đáp ứng các nhu cầu cụ thể của EU; và
- Thu hút giới bảo hiểm đối với việc phát triển các phương pháp và công cụ quản lý rủi ro.

Nguồn: Abridged from Europa, "Strategy for a secure information society (2006 communication)," European Commission, http://europa.eu/scadplus/leg/en/lvb/l24153a.htm

Hội đồng Công ước Châu Âu về tội phạm mạng – CECC (Council of Europe Convention on Cybercrime)

Năm 2001, Liên minh Châu Âu EU đã công bố CECC, cơ quan "đưa ra hướng dẫn cho tất cả các chính phủ có nhu cầu phát triển pháp luật chống tội phạm mạng" và "cung cấp khuôn khổ hợp tác trên phạm vi quốc tế cho lĩnh vực này". 39 quốc gia Châu Âu đã ký vào hiệp ước, ngoài ra còn có Canada, Nhật Bản, Nam Phi và Hoa Kỳ. Điều này khiến cho CECC, có hiệu lực từ tháng 7/2004, "là hiệp ước quốc tế ràng buộc duy nhất được thực hiện cho tới nay"[19].

Cơ quan An ninh Thông tin và Mạng lưới Châu Âu – ENISA (European Network and Information Security Agency)

ENISA được thành lập bởi Quốc hội Châu Âu và Hội đồng EU vào ngày 10/3/2004 "nhằm giúp tăng cường an ninh thông tin và mạng lưới trong cộng đồng (Châu Âu) đồng thời xúc tiến làm nổi bật vai trò của an ninh thông tin và mạng lưới đối với lợi ích của người dân, người tiêu dùng, các doanh nghiệp và các tổ chức hoạt động trong khu vực công".

Tầm nhìn của Nhóm các bên liên quan thường trực (Permanent Stakeholders Group - PSG) về ENISA[20] được đưa ra rõ ràng vào tháng 5/2006 cho thấy ENISA như một trung tâm nổi trội về lĩnh vực an ninh thông tin và mạng lưới, một diễn đàn dành cho các bên liên quan NIS, một nhân tố định hướng nhận thức an ninh thông tin cho toàn bộ dân cư của EU. Để khép lại vấn đề này, các hành động mang tính dài hạn sau đây của ENISA được quy định trong Tầm nhìn PSG (Hình 6):

Hình 6. Hành động mang tính dài hạn của ENISA

Nguồn: (Source: Paul Dorey and Simon Perry, ed. The PSG Vision for ENISA (Permanent Stakeholders Group, 2006), http://www.enisa.europa.eu/doc/pdf/news/psgvisionforenisafinaladoptedmay2006version.pdf)

[19] Council of Europe, "Cybercrime: a threat to democracy, human rights and the rule of law," http://www.coe.int/t/dc/files/themes/cybercrime/default_en.asp

[20] Paul Dorey and Simon Perry, ed. The PSG Vision for ENISA (Permanent Stakeholders Group, 2006), http://www.enisa.europa.eu/doc/pdf/news/psgvisionforenisafinaladoptedmay2006version.pdf

1. Hợp tác và điều phối thẩm quyền an ninh thông tin và mạng lưới quốc gia của các thành viên chính phủ

Hiện tại, sự hợp tác giữa các cơ quan quốc gia rất yếu. Sự việc có thể được thực hiện tốt hơn nhiều thông qua thúc đẩy tăng cường truyền thông và hợp tác giữa các cơ quan quốc gia, đặc biệt là việc chia sẻ những kinh nghiệm tốt từ các cơ quan đi trước với những cơ quan mới bắt đầu.

2. Hợp tác với các viện nghiên cứu

Mục đích của ENISA nên được hướng vào nghiên cứu cơ bản và nhắm tới sự phát triển về mặt kỹ thuật để tập trung và các lĩnh vực có lợi ích lớn nhất đối với việc quản lý rủi ro an ninh có thực trong các hệ thống thực tế. ENISA không nên hỗ trợ cho một nghiên cứu những vấn đề của chính nó, mà thực hiện việc điều chỉnh những ưu tiên và quy trình hiện tại trong các chương trình đã có.

3. Hợp tác với các bên bán phần cứng và phần mềm (vendor)

Các nhà cung cấp phần cứng và phần mềm là những đối thủ cạnh

tranh rõ ràng về quyền lợi và điều này có thể là khó khăn đối với họ khi công khai các bài học thực tiễn với nhau. ENISA có thể đưa ra quan điểm không thiên vị và là một diễn đàn cho các cuộc thảo luận nhạy cảm, trong khi duy trì sức mạnh cần thiết để chống lại hành vi phi cạnh tranh.

Tầm nhìn dài hạn của ENISA tập trung nhiều hơn vào việc tạo lập những công nghệ tin cậy về thông tin và mạng lưới có thể kháng cự lại các loại sâu và những vấn đề khác, thay vì mở rộng số lượng các xu hướng an ninh hiện tại. Điều này có thể đạt được với việc đẩy mạnh các kỹ thuật phát triển phần mềm và kiến trúc đúng, an toàn, tin cậy.

4. Tham gia vào các cơ quan thiết lập tiêu chuẩn

Với cách nhìn để nhận biết và công khai những sáng kiến có giá trị cao, ENISA nên theo dõi và giám sát các chủ đề liên quan đến NIS trong các cơ quan thiết lập tiêu chuẩn, bao gồm cả những gì đi kèm với công việc của rất nhiều cơ quan đại diện và chứng nhận an ninh hiện tại.

5. Tham gia vào quà trình lập pháp thông qua vận động hành lang và đóng góp ý kiến

ENISA nên hoạt động để nâng cao vị trí của một đơn vị tư vấn tin cậy được tham vấn sớm trong quá trình đề xuất và soạn thảo các định hướng cũng như pháp chế khác về các vấn đề liên quan đến NIS.

6. Làm việc với các tổ chức người sử dụng

Thông thường các tổ chức người sử dụng không mấy khi được có mặt trong các cơ quan thiết lập tiêu chuẩn và luật pháp như là các vendor. ENISA có thể mang lại cho các nhóm người dùng cuối sự hiểu biết thông suốt trong công tác xây dựng tiêu chuẩn và cơ hội để tác động vào công việc này.

7. Nhận định và xúc tiến những bài học thực tiễn tốt của các Thành viên chính phủ tới người dùng cuối

ENISA không chỉ bảo vệ các lợi ích của doanh nghiệp mà còn nâng cao sự tin tưởng của người dùng trong việc sử dụng các phương tiện số và Internet.

8. Xây dựng một giải pháp chính trị và kỹ thuật để quản lý nhận dạng

Thiếu sự tin tưởng về Internet là cản trở chính đối với phạm vi rộng lớn các khách hàng hướng tới kinh doanh điện tử. Khả năng có thể kiểm tra một cách đúng đắn về chủ sở hữu của một site, một địa chỉ e-mail, hay một số dịch vụ trực tuyến sẽ là một bước đi lớn để thay đổi và nâng cao sự tin tưởng của người dùng nói chung về Internet. Các giải pháp kỹ thuật trong lĩnh vực này có thể được theo đuổi trong quá trình phát triển ngành, tuy nhiên ENISA có thể hướng tới các chính sách rộng lớn của EU cho vấn đề xác thực các thực thể trực tuyến.

9. Thực hiện cân đối các nỗ lực cho vấn đề an ninh của cả "Thông tin"

và "Mạng lưới"

ENISA nên liên hệ với những nhà cung cấp dịch vụ mạng và Internet (ISP/NSP) lớn nhất để giúp họ nhận diện các bài học thực tiễn tốt nhất đối với lợi ích của doanh nghiệp và người tiêu dùng trên toàn Châu Âu. Điều này là quan trọng bởi các ISP/NSP có thể đóng vai trò then chốt trong việc tăng cường an ninh Internet trên phạm vi rộng. Sự điều phối và hợp tác đủ mạnh của các ISP đang là vấn đề ít được quan tâm ở thời điểm hiện tại.

Nguồn: Source: Abridged from Paul Dorey and Simon Perry, ed. The PSG Vision for ENISA (Permanent Stakeholders Group, 2006), http://www.enisa.europa.eu/doc/pdf/news/psgvisionforenisafinaladoptedmay2006version.pdf.

Chiến lược An ninh thông tin của Hàn Quốc

Mặc dù Hàn Quốc là một trong những quốc gia tiên tiến nhất thế giới về công nghệ thông tin, nhu cầu bảo vệ an ninh thông tin mới chỉ được đề cập gần đây. Năm 2004, Chính phủ Hàn Quốc thông qua Bộ Thông tin và Truyền thông (Ministry of Information and Communication - MIC) đưa ra một Lộ trình An ninh thông tin trung và dài hạn (Medium- and Long-term Information Security Roadmap) nhằm mục tiêu thiết lập một nền tảng an ninh thông tin đảm bảo môi trường kết nối an toàn cho Mạng hội tụ băng rộng (Broadband Convergence

Network) đồng thời nhằm phát triển kỹ thuật an ninh chống lại tình trạng sao chép bất hợp pháp của các thiết bị di động thế hệ kết tiếp. Thêm vào đó, Hàn Quốc đã ký Hiệp ước Seoul - Melbourne nhằm xây dựng sự cộng tác giữa các quốc gia Châu Á Thái Bình Dương để chống thư rác thông qua việc thực thi một hệ thống giám sát thư rác, đối phó về mặt công nghệ, đào tạo và củng cố nhận thức cho người dùng, tăng cường hợp công và tư thông qua chia sẻ thông tin giữa các quốc gia và trao đổi nguồn nhân lực.

Các mục tiêu cụ thể của Lộ trình An ninh thông tin bao gồm: (1) Đảm bảo an toàn hạ tầng mạng lưới; (2) Đảm bảo tính tin cậy của các thiết bị và dịch vụ IT mới; (3) Đẩy mạnh nền tảng an ninh thông tin của Hàn Quốc. Việc thực hiện lộ trình này đòi hỏi nguồn ngân sách 247,89 triệu USD phân bổ trong 4 năm (43 triệu USD trong năm 2005, 55,5triệu USD trong năm 2006 và 80,1 triệu USD trong năm 2008).

Đảm bảo an toàn hạ tầng mạng lưới: Theo Lộ trình, an toàn hạ tầng mạng lưới được đảm bảo thông qua việc phát triển một cấu trúc nền tảng an ninh thông tin cho sự tích hợp và phối hợp giữa rất nhiều hệ thống máy tính không đồng nhất; xây dựng công tác quản lý an ninh DNS thế hệ kế tiếp; và phát triển một cơ chế phân tán mạng lưới nhằm ngăn chặng thiệt hại trong môi trường Mạng hội tụ băng rộng từ mạng phân tán tới các mạng tư nhân và ngược lại.

Đảm bảo tính tin cậy của các thiết bị và dịch vụ IT mới: Một mô hình đánh giá tác động an ninh thông tin có thể đánh giá nguy cơ bị tấn công và các mối đe dọa vật lý, kỹ thuật và quản trị sẽ được phát triển nhằm ngăn chặn hiệu quả các lỗ hổng an ninh thông tin trong các dịch vụ IT mới.

Một thủ tục chứng nhận đối với các mức độ đánh giá an ninh thông tin sẽ được đưa vào sử dụng ở đây. Đối với các dịch vụ IT thế hệ kế tiếp, hệ thống chứng nhận sẽ được nâng cấp bao gồm các bản ghi về giao dịch, quyền hạn, con người và các yếu tố tương tự.

Hơn nữa, một kế hoạch về việc phát triển công nghệ an ninh thông tin đã được xây dựng, bao gồm công nghệ xác thực cho các mạng gia đình, công nghệ nhận diện đầu cuối để ngăn chặn truy nhập bất hợp pháp, công nghệ bảo mật cho dịch vụ thế hệ kế tiếp và công nghệ bảo mật cho nội dung thế hệ kế tiếp.

Tạo lập hạ tầng an ninh thông tin: Lộ trình An ninh thông tin Hàn Quốc bao gồm tầm nhìn cho việc nâng cao công tác điều tiết đáp ứng các nhu cầu của một môi trường truyền thông đang thay đổi và chuẩn bị cho các mối đe dọa trong tương lai. Thứ nhất, Trung tâm dịch vụ xử lý các vấn đề liên quan tới Internet (Internet Incident Response Service Centre) nên được tăng cường để đối phó với các hình thức thâm nhập ngày càng nâng cao và tinh vi. Các hệ thống hợp tác an ninh thông tin trong và ngoài nước nên được củng cố và hỗ trợ chúng đối với hình thức an ninh thông tin nghèo nàn đang được cung cấp. Thứ hai, những vấn đề liên quan đến công nghệ như luật bảo vệ bí mật riêng tư cần được phát triển và một Trung tâm dịch vụ xử lý thư rác (Spam Response Service

Centre) cần được đưa vào hoạt động. Thứ ba, các bộ luật hiện tại về an ninh thông tin cần được cải tiến để đáp ứng các nhu cầu của một môi trường thông tin mọi lúc, mọi nơi, mọi đối tượng (ubiquitous environment). Tương tự như vậy, nhận thức về an ninh thông tin cần được đẩy mạnh thông qua các chiến dịch và các chương trình đào tạo chuyên gia an ninh thông tin.

Chiến lược An ninh thông tin của Nhật Bản[21]

Giữ vững mục tiêu trở thành một 'quốc gia tiên tiến về an ninh thông tin'[22], Nhật Bản đã xác định một bộ chi tiết các mục tiêu, dự án và nguyên tắc cơ bản trong lĩnh vực an ninh thông tin. Hội đồng Chính sách An ninh thông tin (Information Security Policy Council) và Trung tâm An ninh thông tin quốc gia (National Information Security Center - NISC) là các tổ chức hạt nhân đang giám sát tất cả những vấn đề liên quan tới an ninh thông tin diễn ra trên cả nước. Trong lĩnh vực nghiên cứu về các mối đe dọa mạng, Trung tâm Thanh lọc mạng lưới (Cyber Clean Center) được lập ra để phân tích các đặc điểm của các máy tính ma và xây dựng phương pháp đối phó an toàn và hiệu quả.

Chiến lược An ninh thông tin của Nhật Bản được chia ra làm hai phần: (1) Chiến lược quốc gia thứ nhất về An ninh thông tin (First National Strategy on Information Security), được áp dụng một cách tổng quát; và (2) An ninh Nhật Bản YYYY (Secure Japan YYYY). Chiến lược quốc gia thứ nhất về An ninh thông tin chấp nhận nhu cầu đối với tất cả các "thực thể" trong một xã hội IT "để tham gia vào quá trình tạo lập một môi trường sử dụng IT an toàn". Chiến lược chấp nhận các thực thể "mà trên thực tế thông qua và thực hiện các biện pháp như một thành phần của xã hội IT."[23] Những 'thực thể thực thi' này được chia ra làm bốn loại: chính quyền trung ương và địa phương, cơ sở hạ tầng thiết yếu, các doanh nghiệp và các cá nhân. Mỗi loại đều được yêu cầu lập ra các vai trò, kế hoạch và hoạt động cho mình (như trong bảng 4).

Bảng 4. Các vai trò và kế hoạch của mỗi loại dựa trên Chiến lược quốc gia thứ nhất về An ninh thông tin

Loại	Vai trò	Kế hoạch
Chính quyền trung ương và địa phương	Đưa ra "các bài học thực tiễn tốt nhất" về biện pháp an ninh thông tin	Tiêu chuẩn đối với các biện pháp

[21] Được trích từ NISC, Japanese Government's Efforts to Address Information Security Issue (November 2007), http://www.nisc.go.jp/eng/.
[22] Information Security Policy Council, The First National Strategy on Information Security (2 February 2006), 5. http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf.
[23] Ibid., 11.

Cơ sở hạ tầng thiết yếu	Đảm bảo khả năng cung cấp ổn định các dịch vụ như là nền tảng cho các hoạt động kinh tế và sinh sống của xã hội loài người	Kế hoạch hành động cơ sở hạ tầng thiết yếu
Các doanh nghiệp	Thực thi các biện pháp an ninh thông tin được quan tâm cao hơn bởi thị trường	Các biên pháp được xúc tiến bởi các Bộ và Ban ngành
Các cá nhân	Tăng cường nhận thức như là một yếu tố chính trong xã hội IT	Các biên pháp được xúc tiến bởi các Bộ và Ban ngành

Nguồn: NISC, *Japanese Government's Efforts to Address Information Security Issues* (November 2007), http://www.nisc.go.jp/eng/.

Các chính sách thực tiễn trong Chiến lược quốc gia thứ nhất về An ninh thông tin bao gồm như sau:

- Thúc đẩy công nghệ an ninh thông tin – Phát triển công nghệ dành riêng cho chính phủ sử dụng đồng thời thúc đẩy sự phát triển công nghệ giải quyết "Thách thức lớn" (Grand Challenge) trong quá trình đổi mới công nghệ cơ bản với cái nhìn dài hạn.
- Thúc đẩy hợp tác và phối hợp trên phạm vi quốc tế - Góp phần vào sự thiết lập các nền tảng quốc tế về vấn đề an ninh thông tin, đồng thời tạo cho Nhật Bản khả năng dẫn đầu về sự đóng góp trên phạm vi quốc tế.
- Phát triển nguồn nhân lực – Phát triển nguồn nhân lực với năng lực và kỹ năng thực tế cũng như các khả năng rộng lớn, đồng thời tổ chức một hệ thống đủ năng lực cho an ninh thông tin; và
- Biện pháp bảo vệ và kiểm soát sự vi phạm đối với quyền và lợi ích – Tăng cường kiểm soát tội phạm mạng và phát triển các nền tảng pháp luật có liên quan, đồng thời phát triển công nghệ giúp cải thiện an ninh trong môi trường mạng.

An ninh Nhật Bản YYYY (Secure Japan YYYY) là một kế hoạch hàng năm về an ninh thông tin. Secure Japan 2007 là một tài liệu kế hoạch gồm có 159 định hướng và biện pháp thực hiện an ninh thông tin cho 24 vấn đề ưu tiên trong năm 2007. Chúng có thể được tóm tắt lại như sau:

- Nâng cao các biện pháp an ninh thông tin cho các cơ quan chính phủ trung ương;

. Phổ biến các biện pháp cho những đơn vị đi sau để đảm bảo an ninh thông tin, cũng như cho công chúng nói chung; và

. Nỗ lực cao độ nhằm mục tiêu củng cố nền tảng an ninh thông tin.

Câu hỏi suy nghĩ

1. Hoạt động an ninh thông tin tại đất nước bạn khác như thế nào so với những mô tả trên?
2. Có hoạt động an ninh thông tin nào được thực hiện tại các quốc gia đã đề cập trong phân này mà không áp dụng được hay không thích hợp với đất nước bạn? Nếu có thì đó là những hoạt động nào và tại sao lại không áp dụng được hay không thích hợp?

3.2. Các hoạt động an ninh thông tin quốc tế

Các hoạt động an ninh thông tin của tổ chức Liên hợp quốc (United Nations)

Tại Hội nghị thượng đỉnh về Xã hội Thông tin (World Summit on the Information Society - WSIS[24]) được bảo trợ bởi UN, một tuyên bố về các nguyên tắc và kế hoạch hành động cho sự phát triển hiệu quả của xã hội thông tin và thu hẹp 'khoảng cách thông tin' đã được thông qua. Kế hoạch hành động đưa ra một loạt vấn đề sau:

. Vai trò của các chính phủ và tất cả các bên liên quan trong việc thúc đẩy sự phát triển của ICT

. Hạ tầng thông tin và truyền thông được coi là nền tảng thiết yếu cho một xã hội thông tin

. Truy cập thông tin và tri thức

. Xây dựng năng lực

. Xây dựng an ninh và sự tin tưởng trong việc sử dụng ICT

. Ứng dụng ICT trong tất cả các mặt của đời sống

. Tính đồng nhất và đa dạng về văn hóa, tính đa dạng về ngôn ngữ và nội dung bản địa

. Truyền thông media

. Khuôn khổ đạo đức trong Xã hội thông tin

[24] World Summit on the Information Society, "Basic Information: About WSIS," http://www.itu.int/wsis/basic/about.html.

. Hợp tác vùng và hợp tác quốc tế[25]

Diễn đàn Quản trị Internet[26] (Internet Governance Forum – IGF) là tổ chức hỗ trợ UN về các vấn đề quản trị Internet. Nó được thành lập trong trong giai đoạn 2 của WSIS tại Tunis nhằm xác định và giải quyết các vấn đề liên quan đến quản trị Internet. Diễn đàn IGF thứ hai được tổ chức tại Rio de Janeiro từ 12 đến 15 tháng 11 năm 2007, tập trung vào các vấn đề an ninh thông tin như khủng bố mạng, tội phạm mạng và sự an toàn cho trẻ em trong môi trường Internet.

Các hoạt động an ninh thông tin của tổ chức OECD[27]

Tổ chức Phát triển và Hợp tác Kinh tế (Organisation for Economic Co-operation and Development - OECD) là diễn đàn duy nhất, nơi chính phủ của 30 nền dân chủ thị trường làm việc cùng nhau với các doanh nghiệp và cộng đồng để giải quyết các thách thức về kinh tế, xã hội, môi trường và quản trị đang phải đối mặt trong quá trình toàn cầu hóa kinh tế thế giới. Bên trong OECD, Đơn vị hợp tác về An ninh thông tin và Bí mật riêng tư (Working Party on Information Security and Privacy - WPISP) hoạt động dưới sự bảo trợ của Ủy ban Chính sách Thông tin, Máy tính và Truyền thông (Committee for Information, Computer and Communications Policy) nhằm cung cấp các phân tích tác động của ICT đối với an ninh thông tin và bí mật riêng tư, đồng thời phát triển các khuyến nghị chính sách thông qua sự nhất trí để giữ vững niềm tin vào nền kinh tế Internet.

WPISP hoạt động trong lĩnh vực an ninh thông tin: Năm 2002, OECD đưa ra "Hướng dẫn về An ninh cho các mạng lưới và hệ thống thông tin: Hướng tới văn hóa an ninh"[28] nhằm đẩy mạnh "an ninh trong việc phát triển các mạng lưới và hệ thống thông tin, đồng thời thông qua hướng đi mới trong suy nghĩ và hành xử khi sử dụng và tương tác với các mạng lưới và hệ thống thông tin."[29]

Nhằm chia sẻ kinh nghiệm và các bài học thực tiễn về an ninh thông tin, Diễn đàn thế giới về An ninh mạng lưới và các hệ thông thông tin (Global Forum on Information Systems and Network Security) đã được tổ chức năm 2003 và Hội thảo OECD – APEC về An ninh mạng lưới và các hệ thống thông tin (OECD-APEC Workshop on Security of Information Systems and Networks) được tổ chức năm 2005.

WPISP hoạt động về các vấn đề bí mật riêng tư: Hướng dẫn về bảo vệ bí mật riêng tư và trao đổi dữ liệu cá nhân (Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) năm 1980 thể hiện sự nhất trí

[25] World Summit on the Information Society, Plan of Action (12 December 2003), http://www.itu.int/wsis/docs/geneva/official/poa.html.
[26] Internet Governance Forum, http://www.intgovforum.org.
[27] Được trích tại WPISP, "Working Party on Information Security and Privacy" (May 2007).
[28] OECD, OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (Paris: OECD, 2002), http://www.oecd.org/dataoecd/16/22/15582260.pdf.
[29] Ibid., 8.

của thế giới về quản lý thông tin cá nhân trong cả khu vực công và tư. "Quản lý trực tuyến: Sự chỉ dẫn về Chính sách và Thực tiễn" (Privacy Online: OECD Guidance on Policy and Practice) được đưa ra năm 2002, tập trung vào các công nghệ nâng cao bí mật riêng tư, chính sách bí mật riêng tư trực tuyến, sự điều chỉnh và thi hành, cũng như các vấn đề liên quan tới thương mại điện tử. Hiện tại, WPISP đang hoạt động theo Hợp tác thực thi luật bí mật riêng tư (Privacy Law Enforcement Cooperation).

Các hoạt động khác: Năm 1998, OECD đưa ra "Hướng dẫn về chính sách mật mã" và tổ chức Hội nghị Bộ trưởng về xác thực trong thương mại điện tử tại Ottawa. "Nghiên cứu khảo sát về khuôn khổ chính sách và pháp luật cho dịch vụ chứng thực điện tử và chữ ký số tại các quốc gia thành viên OECD" được tiến hành từ năm 2002 đến 2003. Năm 2005, "Sử dụng chứng thực xuyên biên giới cho các quốc gia OECD" dược công bố.

Năm 2004, "Các công nghệ trên nền tảng Sinh trắc học" được soạn thảo, và năm 2005, một nhóm đặc nhiệm về thư rác được hình thành. Những công việc khác đang diễn ra liên quan tới quản lý nhận dạng số, phần mềm gây hại malware, phổ biến công nghệ nhận dạng sóng vô tuyến (radio frequency identification - RFID), hệ thống mạng và cảm biến, và một khuôn khổ chung cho việc thực thi an ninh thông tin và bí mật riêng tư.

Các hoạt động an ninh thông tin của APEC[30]

Tổ chức Hợp tác kinh tế Châu Á Thái Bình Dương APEC (Asia-Pacific Economic Cooperation) đang theo đuổi các hoạt động an ninh thông tin trong khu vực Châu Á Thái Bình Dương thông qua Nhóm hợp tác về Thông tin và Viễn thông TEL (Telecommunication and Information Working Group), bao gồm ba đơn vị: Nhóm chỉ đạo về Tự do hóa (Liberalization Steering Group), Nhóm chỉ đạo về phát triển ICT (ICT Development Steering Group), và Nhóm chỉ đạo về đặc trách an ninh (Security and Prosperity Steering Group).

Đặc biệt là kể từ Hội nghị Bộ trưởng APEC lần thứ 6 về Thông tin và Viễn thông được tổ chức tại Lima, Peru năm 2005, Nhóm chỉ đạo về đặc trách an ninh đã tăng cường các thảo luận về tội phạm mạng và an ninh mạng. Chiến lược An ninh mạng của APEC (APEC Cyber-Security Strategy) đề cập tới việc nâng cao niềm tin của khách hàng trong sử dụng thương mại điện tử, đáp ứng cho thống nhất nỗ lực của rất nhiều quốc gia. Những nỗ lực này bao gồm việc ban hành và thực thi các bộ luật về an ninh mạng, nhất quán với Cam kết hành động chung 55/63[31] của Liên hợp quốc và Hiệp định về Tội phạm mạng

[30] APEC, "Telecommunications and Information Working Group," http://www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html

[31] 'Combating the criminal misuse of information', xác nhận rằng một cải tiến về công nghệ làm gia tăng các hoạt động tội phạm trong thế giới ảo.

(Convention on Cybercrime)[32]. Dự án Xây dựng năng lực thực thi và Sáng kiến Pháp chế tội phạm mạng TEL (TEL Cybercrime Legislation Initiative and Enforcement Capacity Building Project) sẽ hỗ trợ cho các cơ quan trong vấn đề thực thi các bộ luật mới.

Các thành viên APEC cũng phối hợp cùng với Đội ứng khẩn cấp các sự cố về máy tính CERTs (Computer Emergency Response Teams) như một hệ thống phòng thủ cảnh báo sớm chống lại các cuộc tấn công mạng. Hàn Quốc đang hỗ trợ đào tạo nhằm phát triển các quốc gia thành viên, đồng thời các hướng dẫn cho công tác thiết lập và điều hành CERTs đã được phát triển.

Việc bảo vệ người dùng gia đình và các doanh nghiệp SME trước virus và các cuộc tấn công mạng được xem là một ưu tiên và một số công cụ đã được phát triển cho mục đích này. Thông tin đang được cung cấp để làm sao sử dụng Internet một các đảm bảo, và các vấn đề an toàn liên quan đến công nghệ không dây cũng như trao đổi thư điện tử.

Việc giảm thiểu các hình thức lạm dụng thông tin theo hướng phạm tội thông qua chia sẻ thông tin, phát triển các thủ tục và các bộ luật hỗ trợ lẫn nhau, cũng như các biện pháp khác để bảo vệ người dân và doanh nghiệp sẽ tiếp tục là ưu tiên đối với APECTEL. Như một phần trong chương trình hoạt động của mình về các vấn đề an ninh, năm 2007 APECTEL đã phê chuẩn "Hướng dẫn về Chính sách và Phương pháp kỹ thuật đối phó với mạng máy tính ma" (Guide on Policy and Technical Approach against Botnet) và Hội thảo về Hạ tầng thông tin thiết yếu và An ninh mạng (Workshop on Cyber Security and Critical Information Infrastructure).

Các hoạt động An ninh thông tin của ITU[33]

ITU là cơ quan đi đầu Liên hợp quốc về ICT. Trụ sở đặt tại Geneva, Thụy Sĩ, ITU có 191 Chính phủ thành viên và hơn 700 Hội viên và Thành viên trong lĩnh vực.

Vai trò của ITU trong việc giúp đỡ cộng đồng quốc tế trải rộng trên ba lĩnh vực. Lĩnh vực Truyền thông vô tuyến Radiocommunication Sector (ITU-R) tập trung vào công tác quản lý tài nguyên quỹ đạo vệ tinh và phổ tần số vô tuyến quốc tế. Lĩnh vực Tiêu chuẩn hóa Standardization Sector (ITU-T) tập trung vào công tác tiêu chuẩn hóa các dịch vụ và mạng lưới thông tin – truyền thông. Lĩnh vực Phát triển Development Sector (ITU-D) được thiết lập nhằm hỗ trợ việc mở rộng khả năng truy cập bền vững, công bằng tới ICT như là một phương tiện thúc đẩy sự phát triển kinh tế, xã hội rộng rãi hơn. ITU cũng tổ chức các sự kiện TELECOM đồng thời là cơ quan đi đầu trong WSIS.

---

[32] Một Hiệp định được cam kết tại Budapest nhằm duy trì tính toàn vẹn của các hệ thống máy tính thông qua việc xem xét hành vi phạm tội đối với bất kỳ hành động nào vi phạm tính toàn vẹn. Tham khảo tại http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

[33] Được trích tại ITU, "About ITU," http://www.itu.int/net/about/index.aspx

Trong lĩnh vực an ninh mạng, các sáng kiến chủ yếu của ITU gồm có Chương trình hành động WSIS Action Line C.5, Chương trình nghị sự An ninh không gian mạng toàn cầu ITU Global Cybersecurity Agenda và Cổng An ninh không gian mạng ITU Cybersecurity Gateway.

Trọng tâm chính của Chương trình hành động WSIS Action Line C.5 là:

. Bảo vệ hạ tầng thông tin thiết yếu (CIIP);

. Đẩy mạnh sự trao đổi toàn cầu về an ninh không gian mạng;

. Hài hòa luật pháp quốc gia và sự tuân thủ, điều phối luật pháp quốc tế;

. Chống thư rác;

. Phát triển các khả năng theo dõi, cảnh báo và đối phó các vấn đề liên quan;

. Chia sẻ thông tin về đường lối chỉ đạo, các bài học thực tiễn tốt và cách tiếp cận của quốc gia; và

. Bảo vệ người dùng, dữ liệu và bí mật riêng tư.

Chương trình nghị sự An ninh không gian mạng toàn cầu ITU Global Cybersecurity Agenda (GCA) là một khuôn khổ của ITU cho việc hợp tác quốc tế nhằm đề xuất các giải pháp nâng cao an ninh và sự tin cậy trong xã hội thông tin. GCA có 5 trụ chiến lược: khuôn khổ pháp lý, biện pháp kỹ thuật, cấu trúc tổ chức, xây dựng năng lực và hợp tác quốc tế. Các chiến lược này được xây dựng công phu thông qua các mục tiêu sau đây:

. Phát triển một mô hình pháp chế tội phạm mạng có khả năng tương thích và áp dụng trên phạm vi toàn cầu cùng với các biệp pháp pháp lý vùng/quốc gia đã có;

. Tạo lập các chính sách cấu trúc tổ chức theo vùng và quốc gia về tội phạm mạng;

. Thiết lập các kế hoạch hành động và tiêu chuẩn an ninh tối thiểu được chấp nhận trên toàn cầu về hệ thống và các ứng dụng phần mềm;

. Tạo lập một khuôn khổ toàn cầu cho việc theo dõi, cảnh báo và đối phó các vấn đề liên quan nhằm đảm bảo sự điều phối không biến giới về các sáng kiến;

. Tạo lập và tán thành một hệ thống nhận dạng số rộng rãi và các cấu trúc tổ chức cần thiết nhằm đảm bảo sự công nhận các tài liệu số cho các cá nhân không phân biệt ranh giới địa lý;

. Phát triển một chiến lược toàn cầu nhằm hỗ trợ cho việc xây dựng năng lực của cơ quan và con người giúp nâng cao tri thức và sự hiểu biết xuyên suốt lĩnh vực và tất cả những vấn đề được đề cập ở trên; và

. Đưa ra lời khuyên về một khuôn khổ tiềm năng đối với một chiến lược toàn cầu có nhiều bên liên quan về điều phối, đối thoại và hợp tác quốc tế trong tất cả các lĩnh vực đươc đề cập ở trên.

Cổng An ninh không gian mạng ITU Cybersecurity Gateway nhằm cung cấp một nguồn tài nguyên thông tin dễ dàng sử dụng dựa trên các sáng kiến liên quan tới an ninh không gian mạng quốc tế và quốc gia. Nó sẵn sàng cho các tổ chức quốc tế, các doanh nghiệp, các chính phủ và người dân. Các dịch vụ được cung cấp bởi cổng Gateway bao gồm chia sẻ thông tin, theo dõi và cảnh báo, các bộ luật và pháp chế, bí mật riêng tư và công tác bảo vệ, các giải pháp và tiêu chuẩn ngành.

ITU-D cũng đồng thời cũng giám sát Chương trình hợp tác an ninh không gian mạng (ITU Cybersecurity Work Programme), được thiết lập để giúp các quốc gia phát triển công nghệ an ninh không gian mạng ở mức độ cao. Nó cung cấp sự hỗ trợ liên quan tới các vấn đề sau:

. Thiết lập năng lực và chiến lược quốc gia về an ninh không gian mạng và CIIP;

. Thiết lập pháp chế về tội phạm mạng và các cơ chế thực thi phù hợp;

. Thiết lập khả năng theo dõi, cảnh báo và đối phó các vấn đề liên quan;

. Khắc phục khoảng cách tiêu chuẩn hóa liên quan đến an ninh giữa các quốc gia phát triển và đang phát triển;

. Thành lập cơ quan ITU Cybersecurity/CIIP Directory;

. Xây dựng các chỉ số an ninh không gian mạng;

. Khuyến khích các hoạt động hợp tác vùng;

. Hỗ trợ và chia sẻ thông tin với Cổng An ninh không gian mạng ITU Cybersecurity Gateway;

. Đẩy mạnh và tiến xa hơn các hoạt động liên quan.

Các hoạt động khác của ITU-D liên quan đến an ninh không gian mạng đó là tham gia vào các hoạt động cùng với StopSpamAlliance.org, xây dựng năng lực vùng về pháp chế tội phạm mạng và việc tuân thủ, phát triển và phân phối bộ công cụ giảm thiểu botnet[34], các ấn phẩm về tội phạm mạng/an ninh mạng[35], bộ cong cụ về mô hình pháp chế tội phạm mạng cho các quốc gia đang phát triển, và bộ công cụ tự đánh giá an ninh mạng lưới quốc gia.[36]

[34] Suresh Ramasubramanian and Robert Shaw, "ITU Botnet Mitigation Project: Background and Approach" (ITU presentation, September 2007), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit.pdf.
[35] ITU-D Applications and Cybersecurity Division, "Publications," ITU, http://www.itu.int/ITU-D/cyb/publications/.
[36] ITU-D Applications and Cybersecurity Division, "ITU National Cybersecurity / CIIP Self-Assessment Tool," ITU, http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html.

Các hoạt động an ninh thông tin của ISO/IEC

Hệ thống quản lý an ninh thông tin ISMS (Information Security Management System) là tên được đề xuất cho một hệ thống quản lý an ninh thông tin. Nó bao gồm các hệ thống và các quá trình nhằm đảm bảo tính cẩn mật, tính toàn vẹn và tính sẵn sàng của tài sản thông tin trong khi làm giảm thiểu các mối rủi ro đối với an ninh. Chứng nhận ISMS ngày càng phổ biến trên thế giới, là một bước ngoặt trong lịch sử ISMS được tiêu chuẩn hóa trên bình diện quốc tế nhờ việc phát hành hai tài liệu: IS 27001 đưa ra những yêu cầu đối với việc thiết lập một hệ thống ISMS, và IS 17799: 2000, được công bố như IS 17799: 2005 quy định những quy tắc cơ bản đối với thực thi một hệ thống ISMS.

Tiêu chuẩn ISMS trên thực tế là BS 7799, lần đầu tiên được phát triển bởi Viện Tiêu chuẩn Anh quốc (British Standards Institution - BSI) năm 1995 như một quy tắc thực tiễn đối với việc quản lý an ninh thông tin. Năm 1998, chi tiết kỹ thuật cần có đã được phát triển dựa trên tiêu chuẩn này, "quy tắc thực tiễn đối với việc quản lý an ninh thông tin" đã được chuyển thành Phần 1 (Part 1) và chi tiết kỹ thuật cần có trở thành Phần 2 (Part 2). Phần 1 xác định rõ những quy tắc trong quản lý an ninh thông tin, trong khi Phần 2 đưa ra những yêu cầu đối với việc thiết lập một hệ thống ISMS và môt tả quá trình an ninh thông tin (chu trình Kế hoạch – Thực hiện – Kiểm tra – Hành động) đối với sự cải tiến không ngừng về nền tảng của quản lý rủi ro.

Phần 1 được xây dựng thành IS 17799 bởi ISO/IEC JTC 1/SC27 WG1 năm 2000. Từ đó, IS 17799 đã được xem xét lại (với hơn 2000 phê bình đóng góp) và được sửa lại và phiên bản cuối cùng đã chính thức trở thành tiêu chuẩn quốc tế vào tháng 11/2005. IS 17799: 2000 cung cấp 126 tiêu chuẩn so sánh với 10 lĩnh vực quản lý điều hành. IS 17799 được sửa lại năm 2005 đưa ra 11 chủ điểm quản trị và 133 tiêu chuẩn so sánh.

Phần 2 của BS 17799 được xây dựng năm 1999 đã được sử dụng như là tiêu chuẩn cho chứng nhận ISMS. Nó được sửa lại tháng 9/2002 để phù hợp với tiêu chuẩn ISO 9001 và ISO 14001. Tổ chức ISO đã phê chuẩn BS7799 Part 2: 2002 thông qua phương pháp theo dõi nhanh nhằm đáp ứng các yêu cầu đối với ISMS tiêu chuẩn quá quốc tế và đăng ký nó là tiêu chuẩn quốc tế ISO27001 bằng cách sửa đổi nó một chút trong một thời gian ngắn. Những thay đổi nổi bật nhất được thực hiện bao gồm việc thêm nội dung về hiệu lực và chỉnh sửa phần phụ lục.

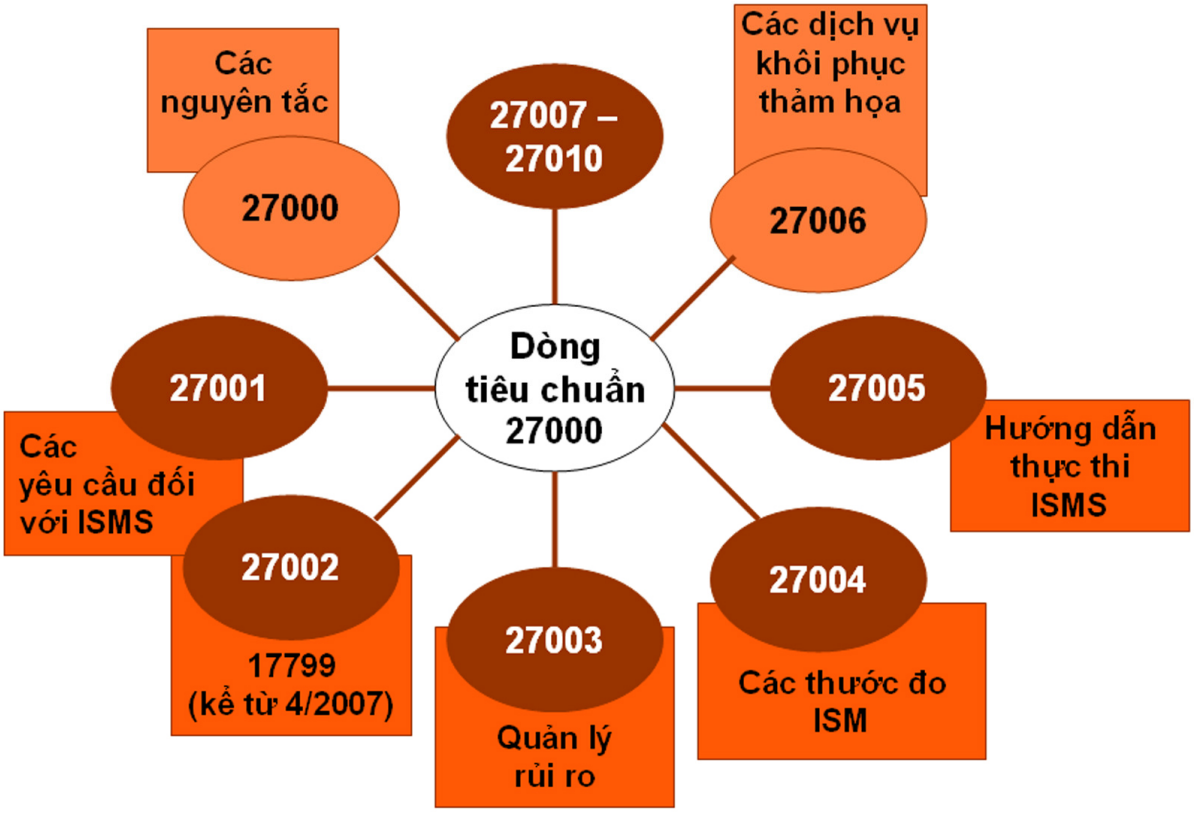
Khi hai tài liệu quan trọng liên quan đến ISMS đã được tiêu chuẩn hóa trên phạm vi quốc tế, một loạt các tiêu chuẩn về an ninh thông tin đã xuất hiện dưới cụm số serial 27000, tương tự như các hệ thống quản lý khác (Chất lượng doanh nghiệp: chuỗi tiêu chuẩn 9000; quản lý các vấn đề môi trường: chuỗi tiêu chuẩn 14000). IS 27001, phiên bản được sửa đổi của IS 17799: 2005, bao gồm các yêu cầu đối với việc thiết lập một hệ thống ISMS và IS 17799: 2005 quy định những quy tắc cơ bản đối với thực thi một hệ thống ISMS đã được chuyển

thành IS27002 vào năm 2007. Hướng dẫn đối với việc thực thi một hệ thống ISMS, một tiêu chuẩn cho quản lý rủi ro an ninh thông tin, và thước đo quản lý hệ thống an ninh thông tin được phát triển bởi JTC1 SC27 là chuỗi tiêu chuẩn 27000.

Hình 7 cho thấy một loạt các tiêu chuẩn liên quan đến ISMS. Các hoạt động chứng nhận ISMS ngày càng tăng mạnh và hy vọng là các tiêu chuẩn ISMS và những chỉ dẫn phù hợp với các ngành cụ thể đang được phát triển dựa trên hệ thống ISMS thông thường, phổ biến. Ví dụ như nỗ lực phát triển những chỉ dẫn ISMS phản ánh các đặc trưng của lĩnh vực truyền thông.

Hình 7. Dòng tiêu chuẩn ISO/IEC 27001

(ANSIL, Roadmap ISO/IEC 2700x, ISMS, Forum Eurosec 2007, http://www.ansil.eu/files/pres-eurosec2007-23052007.pdf)



Câu hỏi suy nghĩ

Những hoạt động an ninh thông tin nào là mũi nhọn của các tổ chức quốc tế đã hoặc đang được phê chuẩn tại đất nước của bạn? Chúng được thực thi như thế nào?

Tự kiểm tra

1. Đâu là sự giống nhau giữa các hoạt động an ninh thông tin được thực hiện bởi các quốc gia đề cập trong phần này? Sự khác nhau giữa chúng là gì?
2. Những ưu tiên về an ninh thông tin nào của các tổ chức quốc tế được đưa ra trong phần này?

4. PHƯƠNG PHÁP AN NINH THÔNG TIN

Phần này nhằm mục tiêu phương pháp an ninh thông tin về mặt kỹ thuật, vật lý và quản trị được sử dụng trên thế giới.

4.1. Phương pháp an ninh thông tin

Phương pháp an ninh thông tin nhằm mục tiêu giảm thiểu thiệt hại và duy trì hoạt động kinh doanh một cách liên tục, tính toán đến tất cả những mối đe dọa và khả năng bị tấn công có thể xảy ra đối với tài sản thông tin. Để chắc chắn hoạt động kinh doanh liên tục, phương pháp an ninh thông tin cố gắng tìm kiếm nhằm đảm bảo tính cẩn mật, tính toàn vẹn và tính sẵn sàng của các tài sản thông tin nội bộ. Điều này đòi hỏi sự gắn kết công tác điều hành và các biện pháp đánh giá rủi ro. Về cơ bản, cần có một kế hoạch tốt có thể kiểm soát an ninh thông tin các khía cạnh kỹ thuật, vật lý và quản trị.

Khía cạnh quản trị

Có rất nhiều hệ thống ISMS tập trung vào khía cạnh quản trị. ISO/IEC27001 là một trong những tiêu chuẩn chung nhất được sử dụng.

ISO/IEC27001, tiêu chuẩn ISMS quốc tế, dựa trên tiêu chuẩn BS7799, được xây dựng bởi BSI. BS7799 đưa ra những yêu cầu đối ới việc quản lý và thực thi một hệ thống ISMS và những tiêu chuẩn chung được áp dụng làm tiêu chuẩn an ninh của rất nhiều các tổ chức và công tác quản lý an ninh hiệu quả. Phần 1 của BS7799 mô tả các hoạt động an ninh cần có dựa trên những bài học thực tiễn tốt nhất về các hoạt động an ninh của tổ chức. Phần 2, hiện tại đã chuyển thành tiêu chuẩn ISO/IEC27001, đề xuất những yêu cầu tối thiểu cần thiết cho công tác vận hành và đánh giá các hoạt động an ninh ISMS.

Các hoạt động an ninh trong ISO/IEC27001 bao gồm 133 tiêu chuẩn so sánh và 11 chủ điểm (bảng 5).

Bảng 5. Các tiêu chuẩn so sánh trong ISO/IEC27001

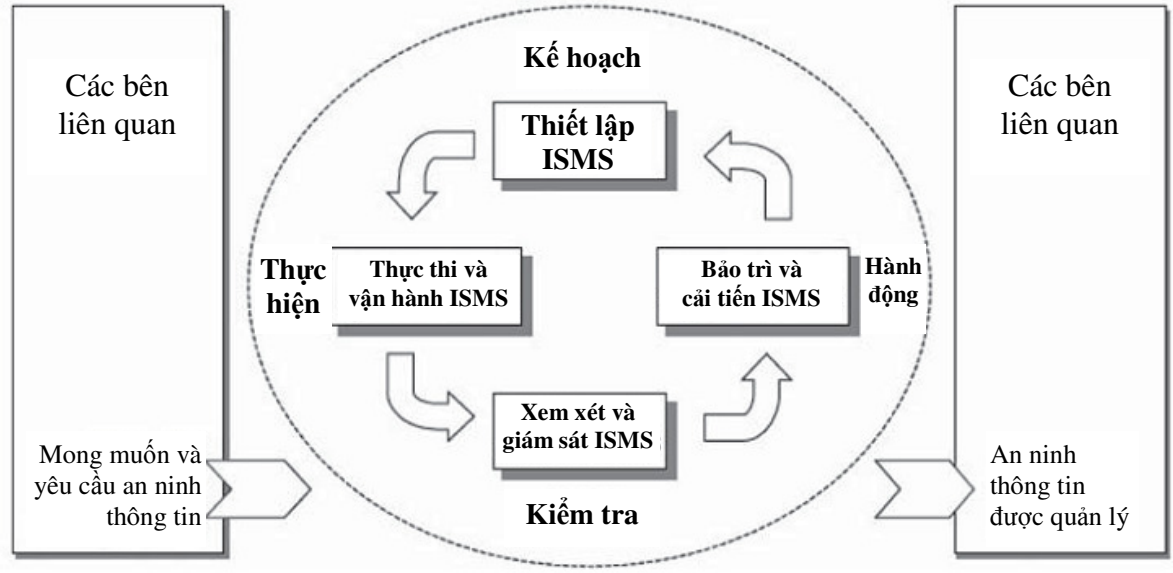
Chủ điểm	Khoản mục
A5	Chính sách an ninh
A6	Tổ chức an ninh thông tin
A7	Quản lý tài sản
A8	An ninh nguồn nhân lực

A9	An ninh khía cạnh môi trường và vật lý
A10	Quản lý vận hành và truyền thông
A11	Quản trị truy cập
A12	Xây dựng,phát triển và bảo trì các hệ thống thông tin
A13	Quản lý các vấn đề gắn liền với an ninh thông tin
A14	Quản lý hoạt động kinh doanh một các liên tục
A15	Sự tuân thủ

ISO/IEC27001 sử dụng mô hình tiến trình Kế hoạch-Thực hiện-Kiểm tra-Hành động (Plan-Do-Check-Act), nó được áp dụng và cấu trúc của tất cả các quá trình trong hệ thống ISMS. Trong ISO/IEC27001, tất cả những dấu hiệu phân tích ISMS đều được ghi chép tài liệu; chứng nhận được kiểm tra định kỳ theo mỗi 6 tháng; và toàn bộ quá trình được lặp lại sau khoảng thời gian 3 năm nhằm quản lý hệ thống ISMS một cách liên tục.

Hình 8. Mô hình quy trình Plan-Do-Check-Act được áp dụng cho các quá trình ISMS

(*Nguồn: ISO/IEC JTC 1/SC 27*)



Các tiêu chuẩn an ninh cần được lên kế hoạch có tính đến các yêu cầu về an ninh. Tất cả nguồn nhân lực, bao gồm các nhà cung cấp, nhà đấu thầu, khách

hàng và các chuyên gia bên ngoài, nên tham gia vào các hoạt động này. Xây dựng các yêu cầu về an ninh được dựa trên ba yếu tố sau:

. Đánh giá rủi ro

. Các điều khoản hợp đồng và yêu cầu luật pháp

. Các quy trình thông tin cho công tác vận hành tổ chức

Phân tích kẽ hở là chỉ quá trình đo đạc mức độ an ninh hiện tại và xây dựng định hướng tương lai cho an ninh thông tin. Kết quả của phân tích kẽ hở nhận được từ những câu trả lời của các chủ sở hữu tài sản cho 133 tiêu chuẩn so sánh và 11 chủ điểm. Một khi những lĩnh vực thiếu hụt được xác định thông qua phân tích kẽ hở, các tiêu chuẩn so sánh thích hợp cho mỗi lĩnh vực có thể được thiết lập.

Đánh giá rủi ro được chia ra thành đánh giá giá trị tài sản và đánh giá khả năng bị tấn công cũng như các mối đe dọa. Đánh giá giá trị tài sản là việc định lượng giá trị các tài sản thông tin. Đánh giá mối đe dọa liên quan đến việc ước tính các mối đe dọa đối với tính cẩn mật, tính toàn vẹn và tính sẵn sàng của thông tin. Ví dụ sau đây sẽ cho thấy việc tính toán có liên quan trong công tác đánh giá rủi ro.

Tên tài sản	Giá trị tài sản	Mối đe dọa			Khả năng bị tấn công			Rủi ro		
		C	I	A	C	I	A	C	I	A
Tài sản #1	2	3	3	1	3	1	1	8	6	5

. Gía trị tài sản + Mối đe dọa + Khả năng bị tấn công = Rủi ro

. Tính cẩn mật: Gía trị tài sản(2) + Mối đe dọa(3) + Khả năng bị tấn công(3) = Rủi ro(8)

. Tính toàn vẹn: Gía trị tài sản(2) + Mối đe dọa(3) + Khả năng bị tấn công(1) = Rủi ro(6)

. Tính sẵn sàng: Gía trị tài sản(2) + Mối đe dọa(1) + Khả năng bị tấn công(1) = Rủi ro(4)

Ứng dụng của các tiêu chuẩn so sánh: Mỗi giá trị rủi ro sẽ khác nhau theo kết quả của công tác đánh giá rủi ro. Quyết định là cần thiết để áp dụng các tiêu chuẩn so sánh thích hợp đối với các tài sản có giá trị khác nhau. Các mối rủi ro được phân chia thành rủi ro có thể chấp nhận được và rủi ro không thể chấp nhận được. Các tiêu chuẩn so sánh được áp dụng dựa trên tiêu chuẩn ISO/IEC, tuy nhiên nó sẽ hiệu quả hơn nếu áp dụng các tiêu chuẩn so sánh dựa trên thực trạng của tổ chức.

Mỗi quốc gia có một cơ quan chứng nhận ISO/IEC27001. Bảng 6 liệt kê số lượng cơ quan chứng nhận theo từng nước.

Bảng 6. Số lượng cơ quan chứng nhận theo quốc gia

Japan	2863*	Netherlands	11	Bulgaria	2
India	433	Singapore	11	Canada	2
UK	368	Philippines	10	Gibraltar	2
Taiwan	202	Saudi Arabia	10	Isle of Man	2
China	174	Pakistan	10	Morocco	2
Germany	108	Russian Federation	10	Oman	2
USA	82	France	9	Qatar	2
Hungary	74	Colombia	7	Yemen	2
Republic of Korea	71	Slovenia	7	Armenia	1
Czech Republic	66	Sweden	7	Bangladesh	1
Italy	54	Slovakia	6	Belgium	1
Hong Kong	38	Croatia	5	Egypt	1
Poland	36	Greece	5	Iran	1
Australia	28	South Africa	5	Kazakhstan	1
Austria	26	Bahrain	4	Kyrgyzstan	1
Ireland	26	Indonesia	4	Lebanon	1
Malaysia	26	Kuwait	4	Lithuania	1
Spain	26	Norway	4	Luxembourg	1
Brazil	20	Sri Lanka	4	Macedonia	1
Mexico	20	Switzerland	4	Moldova	1
Thailand	17	Chile	3	New Zealand	1
Romania	16	Macau	3	Ukraine	1
Turkey	15	Peru	3	Uruguay	1
UAE	14	Portugal	3	**Tổng tương đối**	4997
Iceland	11	Viet Nam	3	**Tổng tuyệt đối**	**4987**

Ghi chú: Số lượng các cơ quan chứng nhận ở đây được tính đến thời điểm 21/12/2008.

Nguồn: International Register of ISMS Certificates, "Number of Certificates per Country," ISMS International User Group Ltd., http://www.iso27001certificates.com.

Khía cạnh vật lý

Hiện tại, chưa có hệ thống quản lý an ninh thông tin về mặt vật lý nào trên phạm vi quốc tế. Tiêu chuẩn 426 của Cục quản lý tình trạng khẩn cấp Liên bang (Federal Emergency Management Agency - FEMA)[37], là tiêu chuẩn về mặt vật lý cho hệ thống ISMS tại Mỹ và rất nhiều quốc gia sử dụng nó như một phương pháp, sẽ được mô tả ở đây.

FEMA 426 đưa ra những chỉ dẫn cho việc xây dựng năng lực bảo vệ chống lại các cuộc tấn công khủng bố. Nó được định hướng tới "việc xây dựng cộng đồng khoa học bao gồm các kỹ sư và kiến trúc sư, nhằm làm giảm thiểu thiệt hại về mặt vật lý tới các công trình liên quan đến cơ sở hạ tầng và con người, gây ra bởi những cuộc tấn công khủng bố."[38] Một loạt các chỉ dẫn liên quan đó là FEMA 427 (Mở đầu cho việc thiết kế các tòa nhà thương mại nhằm giảm thiểu tấn công khủng bố - A Primer for the Design of Commercial Buildings to Mitigate Terrorist Attacks), FEMA 428 (Mở đầu cho việc thiết kế các dự án trường học an toàn trong trường hợp tấn công khủng bố - A Primer to Design Safe School Projects in Case of Terrorist Attacks), FEMA 429 (Mở đầu các khía cạnh Bảo hiểm, Tài chính và Điều tiết đối với việc quản lý rủi ro khủng bố trong các tòa nhà - Insurance, Finance, and Regulation Primer for Terrorism Risk Management in Buildings), FEMA 430 (kiến trúc), and FEMA 438 (tiến trình).

FEMA 426 không liên quan một cách trực tiếp đến an ninh thông tin, tuy nhiên nó có thể ngăn ngừa các kẽ hở, mất hoặc phá hủy thông tin bởi những tấn công về mặt vật lý vào các tòa nhà. Đặc biệt, FEMA 426 liên quan mật thiết với kế hoạch kinh doanh liên tục, là một thành phần của an ninh quản trị. Thông qua việc xem xét FEMA 462, khía cạnh vật lý của kế hoạch kinh doanh liên tục có thể được bảo vệ.

Khía cạnh kỹ thuật

Chưa có hệ thống ISMS đối với khía cạnh kỹ thuật. Các tiêu chuẩn đánh giá chung của thế giới như chứng nhận Common Criteria (CC) có thể được sử dụng thay thế.

Chứng nhận Common Criteria[39]

Chứng nhận CC có nguồn gốc thương mại. Nó được xây dựng để giải quyết những băn khoăn về sự khác biệt mức độ an ninh trong những sản phẩm IT của các quốc gia khác nhau. Tiêu chuẩn quốc tế để định giá các sản phẩm IT được xây dựng bởi Canada, Pháp, Đức, Anh và Mỹ.

---

[37] FEMA, "FEMA 426 - Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings," http://www.fema.gov/plan/prevent/rms/rmsp426.
[38] Ibid.
[39] Common Criteria, http://www.commoncriteriaportal.org.

Một cách cụ thể, CC đưa ra yêu cầu về an ninh IT của một sản phẩm hay hệ thống theo các nhóm khác nhau gồm các yêu cầu về mặt chức năng và yêu cầu về sự bảo đảm. Các yêu cầu về chức năng của CC định rõ hành động an ninh được đề nghị. Các yêu cầu về sự bảo đảm là cơ sở cho việc gia tăng sự tin tưởng theo đó các biện pháp an ninh được đòi hỏi phải hiệu quả và được thực thi một cách đúng đắn. Chức năng an ninh CC bao gồm 136 thành phần từ 11 lớp tạo nên 57 nhóm. Các yêu cầu về sự bảo đảm đưa ra 86 thành phần từ 9 lớp và tạo nên 40 nhóm.

Các yêu cầu về chức năng an ninh (Security functional requirement - SFR): SFR xác định tất cả các chức năng an ninh cho việc Đánh giá Mục tiêu (Target of Evaluation - TOE). Bảng 7 liệt kê các lớp chức năng an ninh có trong SFR.

Bảng 7. Thành phần kết cấu của lớp trong SFR

Các lớp		Chi tiết
FAU	Kiểm tra an ninh	Chỉ ra những chức năng bao gồm kiểm tra việc bảo vệ dữ liệu, lựa chọn sự kiện và định dạng bản ghi, cũng như các công cụ phân tích, phân tích thời gian thực và cảnh báo xâm phạm
FCO	Truyền thông	Mô tả những yêu cầu một cách cụ thể có liên quan tới TOE mà được sử dụng cho việc truyền tải thông tin
FCS	Hỗ trợ mật mã	Chỉ rõ việc sử dụng quản lý mã khóa và sử dụng mật mã
FDP	Bảo vệ dữ liệu người dùng	Xác định các yêu cầu liên quan tới bảo vệ dữ liệu người dùng
FIA	Nhận diện và xác thực	Xác định các yêu cầu về chức năng để thiết lập và kiểm tra một đối tượng người dùng
FMT	Quản lý an ninh	Chỉ rõ việc quản lý một số khía cạnh của Các chức năng an ninh TOE (TOE Security Functions - TSF): các thuộc tính an ninh, các chức năng và dữ liệu TOE
FPR	Bí mật riêng tư	Mô tả những yêu cầu có thể được chọn lựa để đáp ứng nhu cầu bí mật riêng của người dùng, trong khi vẫn linh hoạt cho phép hệ thống có thể duy trì khả năng kiểm soát toàn bộ hoạt động vận hành
FPT	Bảo vệ TSF	Bao gồm các nhóm yêu cầu về chức năng liên quan đến tính toàn vẹn và công tác quản lý các cơ chế

		cấu thành TSF cũng như tính toàn vẹn của dư liệu TSF
FRU	Tận dụng nguồn lực	Bao gồm tính sẵn sàng của các nguồn lực cần thiết như khả năng xử lý và/hoặc khả năng lưu trữ
FTA	Truy nhập TOE	Xác định các yêu cầu chức năng đối với việc kiểm soát sự thiết lập một phiên truy nhập
FTP	Các kênh/tuyến tin cậy	Cung cấp các yêu cầu đối với một tuyến liên lạc tin cậy giữa người dùng và TSF

Nguồn: Common Criteria, Common Methodology for Information Technology Security Evaluation, 9/2007, CCMB-2007-09-004

Các thành phần của việc đảm bảo an ninh (Security assurance components - SACs): Triết lý CC đòi hỏi sự gắn kết các mối đe dọa an ninh và việc phê chuẩn chính sách an ninh về mặt tổ chức thông qua các biện pháp an ninh tương xứng và thích hợp. Những biện pháp được phê chuẩn sẽ giúp nhận diện các khả năng bị tấn công, giảm khả năng khai thác bị tận dụng và giảm sự mở rộng về thiệt hại trong tình huống một khả năng tấn công bị lợi dụng.[40] Bảng 8 liệt kê các lớp có trong SACs.

Bảng 8. Thành phần kết cấu của lớp trong SACs

Các lớp		Chi tiết
APE	Đánh giá Hồ sơ bảo vệ (Protection Profile - PP)	Điều này được yêu cầu nhằm chứng tỏ rằng PP đúng đắn và nhất quán bên trong, đồng thời, nếu PP được dựa trên một hay nhiều PP khác thì đó là một thuyết minh đúng đắn cho những PP này
ASE	Đánh giá Mục tiêu an ninh (Security Target - ST)	Điều này được yêu cầu nhằm chứng tỏ rằng ST đúng đắn và nhất quán trong, đồng thời, nếu ST được dựa trên một hay nhiều ST khác thì đó là một thuyết minh đúng đắn cho những ST này
ADV	Sự phát triển	Cung cấp thông tin về TOE. Các kiến thức thu được được sử dụng như là nền tảng cho việc chỉ đạo công tác phân tích khả năng bị tấn công và kiểm thử dựa trên TOE, được mô tả trong lớp ATE và AVA

[40] Common Criteria, Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements (August 1999, Vesion 2.1), http://www.scribd.com/doc/2091714/NSA-Common-Critira-Part3.

AGD	Tài liệu hướng dẫn	Để đảm bảo cho công tác chuẩn bị và vận hành TOE, cần phải mô tả tất cả những khía cạnh liên quan tới việc đảm bảo sự kiểm soát của TOE. Nhóm cũng xác định các khả năng sai sót không định trước trong cấu hình và kiểm soát TOE
ALC	Hỗ trợ vòng đời sản phẩm	Trong vòng đời sản phẩm, bao gồm các năng lực quản lý cấu hình (configuration management - CM), phạm vi CM, sự phân phát, phát triển an ninh, việc bù đắp các chỗ hổng, xác định vòng đời, các công cụ và kỹ thuật, nó xác định TOE có thuộc trách nhiệm của người phát triển hoặc người sử dụng hay không
ATE	Kiểm thử	Tầm quan trọng của lớp này thể hiện bằng việc xác nhận rằng TSF vận hành theo đúng những mô tả thiết kế của nó. Nhóm này không thực hiện việc kiểm thử xâm nhập
AVA	Đánh giá khả năng bị tấn công	Hoạt động đánh giá khả năng bị tấn công bao quát rất nhiều khả năng bị tấn công trong quá trình vận hành và phát triển TOE
ACO	Kết cấu	Xác định các yêu cầu về sự bảo đảm được thiết kế nhằm mang lại sự tin cậy mà một TOE có sẽ vận hành một cách an toàn khi tin tưởng vào chức năng an ninh được cung cấp bởi rất nhiều thành phần phần cứng, firmware, phần mềm đánh giá

Nguồn: Common Criteria, Common Methodology for Information Technology Security Evaluation, 9/2007, CCMB-2007-09-004

Phương pháp đánh giá của CC

Đánh giá PP: PP mô tả các bộ thực thi độc lập của các yêu cầu an ninh cho nhiều loại TOE và bao gồm một báo cáo về vấn đề an ninh mà một sản phẩm được dự định để giải quyết. Nó xác định các yêu cầu về chức năng và sự bảo đảm của CC, và đưa ra cơ sở hợp lý cho việc lựa chọn các thành phần bảo đảm và thành phần chức năng. Nó được tạo nên bởi một khách hàng hay nhóm khách hàng có các yêu cầu an ninh IT.

Đánh giá ST: ST là cơ sở cho việc thỏa thuận giữa những nhà phát triển TOE, người tiêu dùng, người đánh giá và các cơ quan đánh giá như những gì TOE cung cấp, cũng như phạm vi của việc đánh giá. Sự hiện diện của một ST có thể cũng bao gồm việc quản lý, tiếp thị, mua sắm, cài đặt, cấu hình, vận hành và sử dụng TOE. Một ST bao gồm một số việc thực thi thông tin nhất định, thể hiện

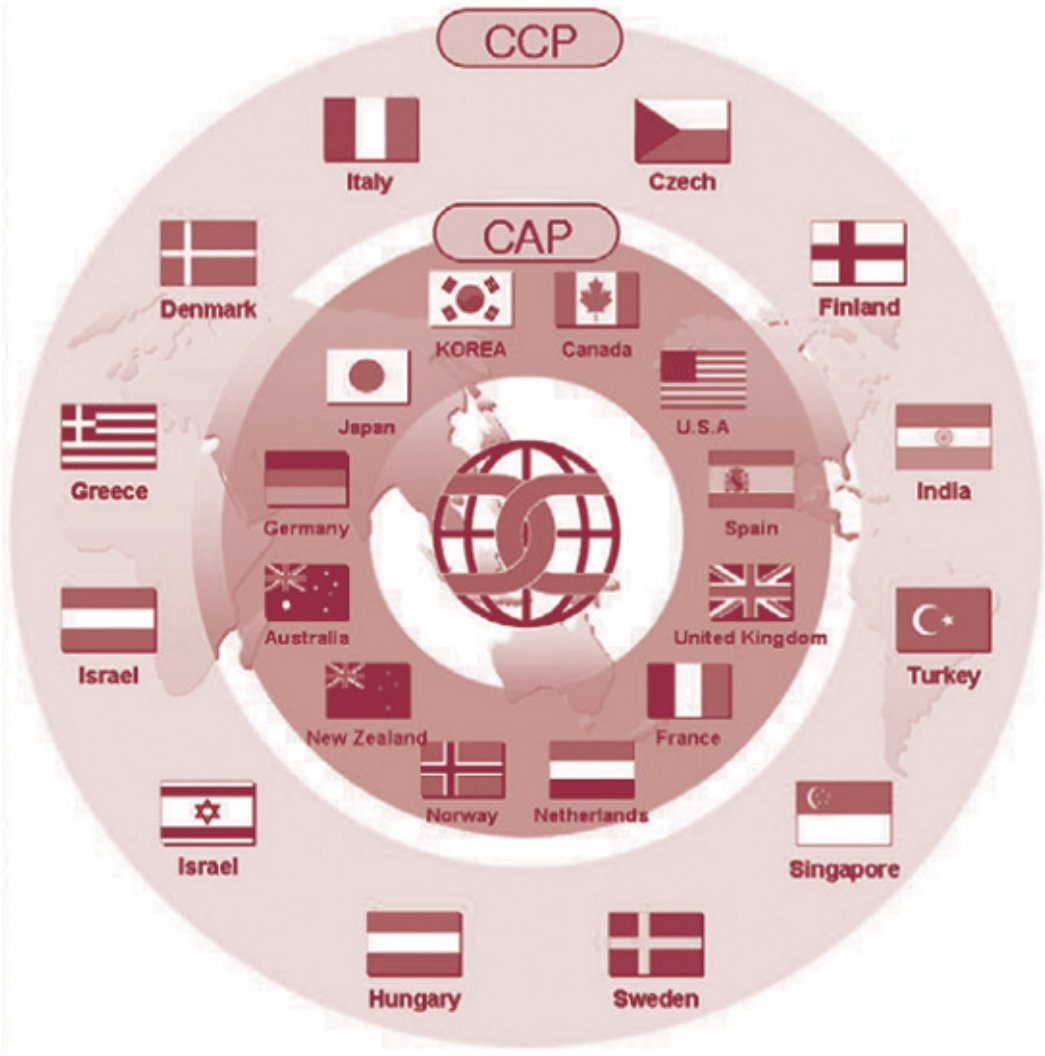
sản phẩm xử lý các yêu cầu an ninh như thế nào. Nó có thể dẫn tới một hoặc nhiều PP. Trong trường hợp này, ST phải thực hiện đầy đủ các yêu cầu an ninh chung được định rõ trong mỗi PP và có thể xác định những yêu cầu xa hơn.

Tổ chức công nhận về tiêu chí chung

Tổ chức công nhận về tiêu chí chung (Common Criteria Recognition Arrangement - CCRA) được xây dựng để phê chuẩn chứng nhận CC giữa các quốc gia. Nó nhằm mục tiêu đảm bảo rằng những đánh giá CC được thực hiện với các tiêu chuẩn nhất quán, loại trừ hoặc giảm thiểu những đánh giá trùng lặp đối với các sản phẩm IT hay hồ sơ bảo vệ, và nâng cao các cơ hội thị trường toàn cầu trong lĩnh vực IT thông qua việc phê chuẩn chứng nhận giữa các quốc gia thành viên.

CCRA gồm có 24 quốc gia thành viên, trong đó 12 thành viên là Cơ quan cấp quyền chứng nhận (Certificate Authorizing Participants - CAPs) và 12 là Cơ quan thực thi chứng nhận (Certificate Consuming Participants - CCPs). CAP là những đơn vị đưa ra các chứng nhận đánh giá. Họ là những nhà bảo trợ cho hoạt động của một đơn vị chứng nhận dưới quyền trong nước đồng thời họ cũng thực hiện ủy quyền cấp chứng nhận. Một quốc gia phải là thành viên của CCRA như là CCP với thời hạn tối thiểu là 2 năm trước khi có thể trở thành một CAP. CCP là những đơn vị tiêu thụ các chứng nhận đánh giá. Mặc dù họ có thể không duy trì năng lực đánh giá an ninh IT, họ có một mối quan tâm thực sự về việc sử dụng hồ sơ bảo vệ và các sản phẩm được chứng nhận/phê chuẩn. Để trở thành thành viên của CCRA, một quốc gia phải đệ trình đơn xin tới Ủy ban Quản lý (Management Committee).

Hình 9. CAP và CCP



4.2. Một số ví dụ về phương pháp an ninh thông tin

Viện quốc gia về Công nghệ và Tiêu chuẩn Mỹ (US National Institute of Standards and Technology – NIST)

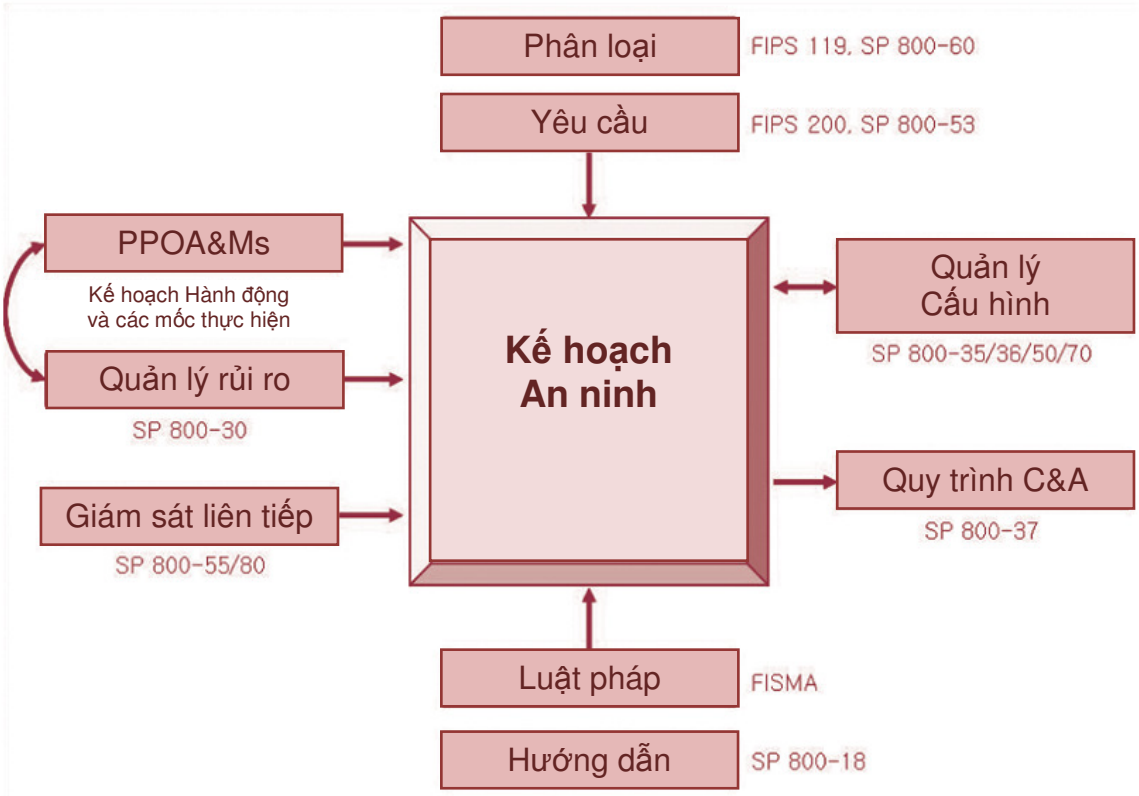
Dựa trên FISMA, NIST đã phát triển các tiêu chuẩn và hướng dẫn cho việc tăng cường an ninh đối với thông tin và những hệ thống thông tin mà các cơ quan Liên bang có thể sử dụng. Các tiêu chuẩn và hướng dẫ nhằm mục tiêu:

- Đưa ra một chỉ định rõ ràng về những yêu cầu an ninh tối thiểu thông qua việc phát triển các tiêu chuẩn có thể được sử dụng để phân loại thông tin và các hệ thống thông tin của Liên bang;
- Cho phép việc phân loại an ninh về thông tin và các hệ thống thông tin;
- Chọn và chỉ định biện pháp kiểm soát an ninh đối với những hệ thống thông tin hỗ trợ cho các cơ quan thực thi của chính quyền Liên bang; và

. Kiểm tra hiệu lực, hiệu quả của các biện pháp an ninh đối với những khả năng bị tấn công.

Những chỉ dẫn có liên quan tới FISMA được công bố như các hình thức xuất bản đặc biệt của Tổ chức Công bố Tiêu chuẩn xử lý thông tin Liên bang (Federal Information Processing Standards Publications). Có hai dòng (series) của hình thức xuất bản đặc biệt: 500 series cho công nghệ thông tin và 800 series cho an ninh máy tính. Hình 10 cho thấy tiến trình mà các cơ quan chính phủ Mỹ tuân theo để thiết lập các kế hoạch an ninh dựa trên tiêu chuẩn này.

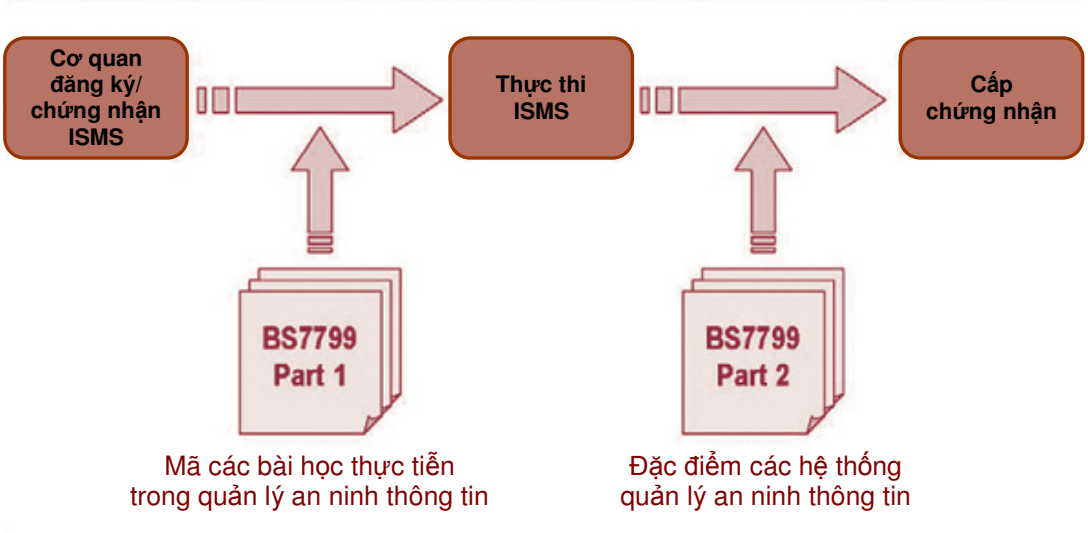
Hình 10. Quy trình hoạch định an ninh đầu vào/đầu ra



Tại Anh (BS7799)

Như đã đề cập từ trước, BSI phân tích hoạt động an ninh của các tổ chức tại Anh và cấp chứng nhận BS7799, hiện tại đã được phát triển thành tiêu chuẩn ISO27001 (BS7799 Part 2) và ISO27002 (BS7799 Part 1). Hình 11 thể hiện quy trình thủ tục được tuân thủ.

Hình 11. Quy trình chứng nhận BS7799



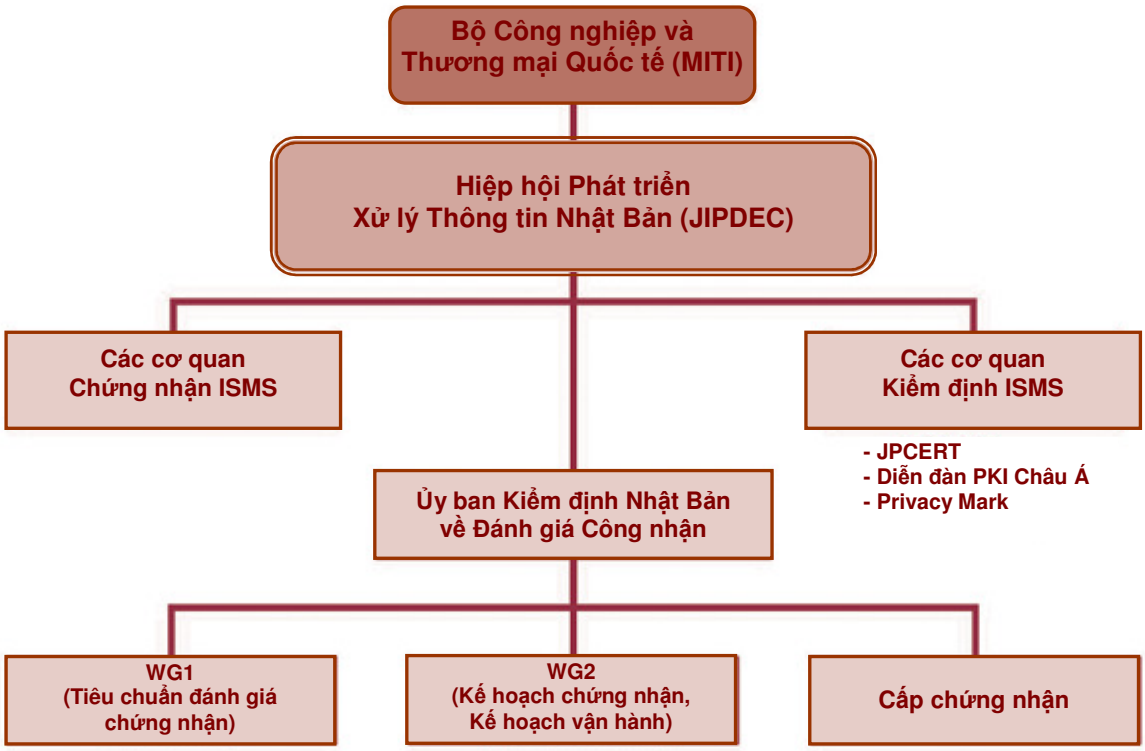
Tại Nhật Bản (từ ISMS Ver2.0 đến BS7799 Part 2: 2002)

ISMS Ver2.0 của Hiệp hội Phát triển Xử lý Thông tin Nhật Bản (Japan Information Processing Development Corporation - JIPDEC) được sử dụng tại Nhật kể từ tháng 4/2002. Gần đây nó được thay thế bởi BS7799 Part 2: 2002.

Tỉ lệ các ứng dụng cho việc cấp chứng nhận đã tăng lên kể từ khi chính quyền trung ương đẩy mạnh kế hoạch an ninh thông tin. Các chính quyền địa phương đã hỗ trợ cho các tổ chức số tiền tài trợ để đạt được chứng nhận ISMS. Tuy nhiên ISMS Ver2.0 chỉ đơn thuần nhấn mạnh khía cạnh quản trị và không bao hàm khía cạnh kỹ thuật của an ninh thông tin. Hơn nữa, hầu hết các tổ chức chỉ quan tâm tới việc được cấp chứng nhận mà không nhất thiết thực hiện việc cải tiến các hoạt động an ninh thông tin của mình.

Hình 12 thể hiện hệ thống chứng nhận ISMS của Nhật Bản.

Hình 12. Chứng nhận ISMS ở Nhật Bản

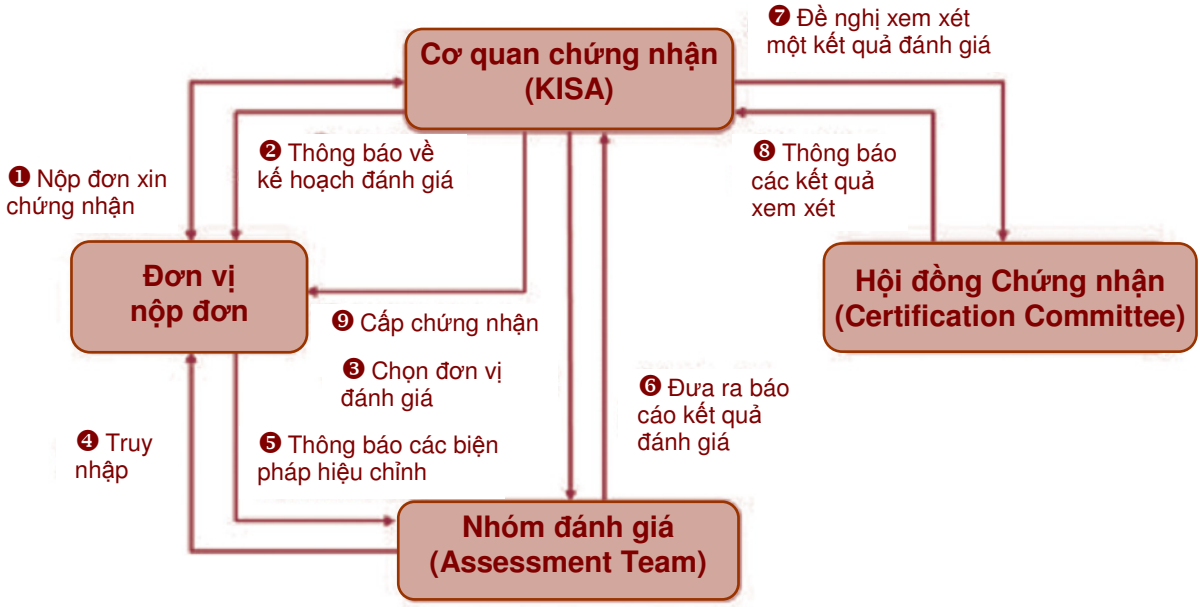


Tại Hàn Quốc (ISO/IEC27001 và/hoặc KISA ISMS)

Chứng nhận ISMS của Cơ quan An ninh thông tin Hàn Quốc (Korea Information Security Agency - KISA) được phát triển chủ yếu bởi Bộ Thông tin và Truyền Thông (MIC) đã được sử dụng trong khi tiêu chuẩn ISO/IEC 27001 đang bắt đầu phổ biến bởi BSI-Korea. ISMS của KISA là một hệ thống quản lý tổng hợp, bao hàm một kế hoạch an ninh vật lý/kỹ thuật. Do đó, hệ thống chứng nhận KISA ISMS củng cố cho lĩnh vực an ninh thông tin về mặt kỹ thuật mà không có trong tiêu chuẩn ISO/IEC27001. Đặc biệt, việc phê chuẩn "Thủ tục An toàn" (Safety Procedure) được coi như một yêu cầu của chứng nhận làm vững chắc công tác kiểm tra về mặt kỹ thuật. Hình 13 cho thấy quy trình chứng nhận của KISA ISMS.

Hình 13. Chứng nhận ISMS của KISA

(Nguồn: KISA, "Procedure of Application for ISMS Certification" (2005), http://www.kisa.or.kr/index.jsp)



Tại Đức (Năng lực bảo hộ lĩnh vực IT - IT Baseline Protection Qualification)

BSI tại Đức (Bundesamt fűr Sicherheit in der Informationstechnik) là cơ quan quốc gia về an ninh thông tin. Nó cung cấp các dịch vụ an ninh IT cho cơ quan Chính phủ, các thành phố, các tổ chức và người dân Đức.

BSI đã xây dựng Năng lực bảo hộ lĩnh vực IT dựa trên tiêu chuẩn quốc tế, ISO Guide 25[GUI25] và tiêu chuẩn Châu Âu EN45001, được thừa nhận bởi Hội đồng Chứng nhận và Kiểm thử IT Châu Âu (European Committee for IT Testing and Certification). Các loại chứng nhận bao gồm IT Baseline Protection Certificate, Self-declared (IT Baseline Protection ở mức độ cao hơn) và Self-declared (IT Baseline Protection ở mức độ cơ bản).

Thêm vào đó, Thông tin hướng dẫn bảo hộ lĩnh vực (Baseline protection manual - BPM) và phụ mục hướng dẫn chuỗi tiêu chuẩn BSI Standard Series:100-X đã được phát triển, chủ yếu bao gồm các phân tích: BSI Standard 100-1 ISMS, BSI Standard 100-2 BPM Methodology và BSI Standard 100-3 Risk.[41]

Tại các quốc gia khác

Bảng 9 liệt kê một số chứng nhận ISMS hiện có tại một số quốc gia khác

Bảng 9. Chứng nhận ISMS của một số quốc gia khác

[41] Antonius Sommer, "Trends of Security Strategy in Germany as well as Europe" (presentation made at the 2006 Cyber Security Summit, Seoul, Republic of Korea, 10 April 2006), http://www.secure.trusted-site.de/download/newsletter/vortraege/KISA.pdf.

Cơ quan chứng nhận		Tiêu chuẩn
Canada	Tổ chức Thiết lập An ninh Truyền thông (Communications Security Establishment)	MG-4, Hướng dẫn Chứng nhận và Kiểm định cho các Hệ thống IT
Đài Loan	Cục Tiêu chuẩn, Khí tượng và Thanh tra (Bureau of Standards, Meteorology and Inspection)	CNS 17799 & CNS 17800
Singapore	Hội đồng Tiêu chuẩn Công nghệ Thông tin (Information Technology Standards Committee)	SS493 : Part1 – Khuôn khổ Tiêu chuẩn An ninh IT (IT Security Standard Framework) & SS493 : Part 2 – Các dịch vụ An ninh (Security Services) cho sự phát triển

5. BẢO VỆ BÍ MẬT RIÊNG TƯ

Phần này nhằm mục đích:

- **Phác họa sự thay đổi trong khái niệm bí mật riêng tư;**
- **Mô tả các xu hướng quốc tế về bảo vệ bí mật riêng tư; và**
- **Đưa ra cái nhìn tổng quan và một số ví dụ về Đánh giá tác động bí mật riêng tư.**

5.1. Khái niệm bí mật riêng tư

Thông tin cá nhân là bất kỳ thông tin nào có liên quan tới khả năng nhận biết một cá thể[42] hoặc khả năng nhận biết hay nhận dạng một con người tự nhiên (thể nhân).[43] Nó bao gồm thông tin như tên, số điện thoại, địa chỉ, địa chỉ e-mail, số giấy phép đăng ký ô tô, các đặc điểm vật lý (các kích thước khuôn mặt, dấu vân tay, chữ viết tay, v.v…) số thẻ tín dụng và mối quan hệ gia đình của một cá nhân.

Việc tiếp cận và thu thập, phân tích và sử dụng một cách không thích hợp thông tin cá nhân của một người có tác động tới hành vi của các đối tượng khác trong quan hệ với cá nhân đó, và cuối cùng có một ảnh hưởng tiêu cực đến vị trí xã hội, tài sản và sự an toàn của ông ấy/bà ấy. Chính vì vậy, thông tin cá nhân cần được bảo vệ trước sự tiếp cận, thu thập, lưu trữ, phân tích và sử dụng trái phép. Theo nghĩa này, thông tin cá nhân là một chủ đề của công tác bảo vệ.

Khi chủ đề của công tác bảo vệ là quyền đối với thông tin cá nhân hơn là bản thân thông tin đó thì đây lại là khái niệm về bí mật riêng tư. Có 5 cách giải thích về quyền bí mật riêng tư:

- Quyền được tự do truy cập (ví dụ truy cập qua các phương tiện vật lý, truy cập qua dịch vụ nhắn tin ngắn)
- Quyền không cho phép thông tin cá nhân bị sử dụng theo cách không mong muốn (ví dụ bán thông tin, công khai thông tin)
- Quyền không cho phép thông tin cá nhân bị thu thập bởi các đối tượng khác mà không có sự đồng ý hay xin phép (ví dụ thông qua việc sử dụng CCTV và cookies)

[42] Cabinet Office, Privacy and Data-sharing: The way forward for public services (April 2002), http://www.epractice.eu/resource/626.

[43] EurLex, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Directive&an_doc=1995&nu_doc=46.

. Quyền được bày tỏ thông tin cá nhân một cách đúng đắn, chính xác (tính chính trực)

. Quyền được khen thưởng cho giá trị thông tin của mình

Khái niệm bị động của bí mật riêng tư bao hàm quyền được tôn trọng và quyền tự nhiên liên quan tới phẩm giá của con người. Nó được gắn với luật chống xâm phạm.

Khái niệm chủ động của bí mật riêng tư bao hàm tự kiểm soát thông tin cá nhân hay quyền quản lý/kiểm soát thông tin cá nhân một cách tuyệt đối, trong đó có quyền hiệu chỉnh để tác động đến kết quả do thông tin cá nhân không chính xác.

5.2. Các xu hướng của chính sách bí mật riêng tư

Hướng dẫn của OECD về bảo vệ bí mật riêng tư

Năm 1980, OECD đã đưa ra Hướng dẫn về bảo vệ bí mật riêng tư và trao đổi dữ liệu cá nhân (Guidelines on the Protection of Privacy and Transborder Flows of Personal Data), cũng được biết đến với tên gọi "OECD Fair Information Practices". Năm 2002, "Bí mật riêng tư trực tuyến: Hướng dẫn của OECD về chính sách và thực tiễn" (Privacy Online: OECD Guidance on Policy and Practice) đã được công bố.[44] Các hướng dẫn áp dụng cho dữ liệu cá nhân, dù trong các lĩnh vực công cộng hay tư nhân, mà gây nguy hiểm đối với bí mật riêng tư và quyền tự do cá nhân do cách thức thông tin được xử lý, hoặc do bản chất hay bối cảnh mà nó được sử dụng. Các nguyên tắc của OECD được xác định trong Hướng dẫn phác thảo quyền và nghĩa vụ của các cá nhân trong bối cảnh tự động xử lý dữ liệu cá nhân, cũng như quyền và nghĩa vụ của những người tham vào quá trình xử lý. Hơn nữa, các nguyên tắc cơ bản được phác thảo trong Hướng dẫn có thể áp dụng cả trên phạm vi trong nước và quốc tế.

8 nguyên tắc tạo nên Hướng dẫn của OECD về bảo vệ bí mật riêng tư là:

1. Nguyên tắc hạn chế thu thập

Cần có các giới hạn đối với việc thu thập dữ liệu cá nhân, và bất kỳ dữ liệu đó phải được thu thập thông qua những cách thức hợp pháp và ngay thẳng, tại địa điểm thích hợp, có sự đồng ý hay xin phép về dữ liệu.

2. Nguyên tắc về chất lượng dữ liệu

Dữ liệu cá nhân cần gắn với các mục đích mà chúng được sử dụng, đồng thời phạm vi của các các mục đích này cần phải rõ ràng, đầy đủ và cập nhật.

3. Nguyên tắc xác định rõ mục đích

[44] OECD, "Privacy Online: OECD Guidance on Policy and Practice," http://www.oecd.org/document/49/0,3343,en_2649_34255_19216241_1_1_1_1,00.html.

Mục đích đối với dữ liệu cá nhân được thu thập cần phải xác định chậm nhất tại thời điểm tiến hành thu thập dữ liệu và việc sử dụng sau đó bị giới hạn theo sự đầy đủ của các mục đích hay các yếu tố khác mà không trái với mục đích, cũng như những gì được xác định theo mỗi lần thay đổi mục đích.

4. Nguyên tắc giới hạn sử dụng

Dữ liệu cá nhân cần đảm bảo không bị công bố, tạo sự sẵn sàng hay được sử dụng cho những mục đích khác ngoài những mục tiêu xác định theo nguyên tắc xác định rõ mục tiêu trừ khi có sự đồng ý của đối tượng dữ liệu hoặc sự cho phép của luật pháp.

5. Nguyên tắc bảo đảm an ninh

Dữ liệu cá nhân cần được bảo vệ bằng các biện pháp an ninh hợp lý nhằm chống lại những hiểm họa như mất hay truy cập trái phép, phá hoại, sử dụng, chỉnh sửa hay phơi bày dữ liệu.

6. Nguyên tắc mở

Cần có một chính sách chung đối với tính công khai về sự phát triển, thực tiễn và các chính sách liên quan tới dữ liệu cá nhân.

7. Nguyên tắc tham gia của cá nhân

Một cá nhân cần có quyền sau:

a. Xác nhận xem một đơn vị điều khiển dữ liệu có các thông tin liên quan đến người đó hay không;

b. Tiếp nhận thông báo về dữ liệu liên quan đến bản thân trong một thời điểm hợp lý, với một mức giá, nếu có, và theo một hình thức dễ hiểu đối với người đó;

c. Được cung cấp lý do nếu một yêu cầu được đưa ra theo các điểm (a) và (b) bị từ chối, và có thể không thừa nhận những từ chối đó; và

d. Có quyền không thừa nhận dữ liệu liên quan đến bản thân, và nếu việc không thừa nhận thành công, dữ liệu phải được xóa, sửa đổi, hoàn thiện hoặc cải tạo.

8. Nguyên tắc trách nhiệm

Một đơn vị điều khiển dữ liệu phải có trách nhiệm đối với việc tuân thủ các biện pháp mang lại hiệu quả cho những nguyên tắc được nêu ở trên.[45]

Hướng dẫn của Liên hợp quốc (UN) có liên quan đến bảo vệ bí mật riêng tư

[45] Có thể đọc toàn văn về những nguyên tắc được trình bày tại: "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

Từ cuối những năm 1960, thế giới đã chú ý đến ảnh hưởng của quá trình xử lý thông tin tự động đến bí mật riêng tư. Đặc biệt, UNESCO đã thể hiện sự quan tâm tới bí mật riêng tư và bảo vệ bí mật riêng tư khi "Hướng dẫn của UN về Công tác điều tiết Tệp tin dữ liệu cá nhân được lưu trư trong máy tính" (UN Guidelines for the Regulation of Computerized Personal Data File) được thông qua bởi Đại Hội đồng năm 1990.

Hướng dẫn của UN áp dụng cho các tài liệu (giấy tờ) cũng như những tệp tin dữ liệu được lưu trữ trong máy tính trong cả lĩnh vực công cộng và tư nhân. Hướng dẫn đưa ra một chuỗi những nguyên tắc liên quan đến sự đảm bảo tối thiểu được đưa ra trong luật pháp quốc gia hay nội quy của các tổ chức quốc tế như sau:

1. Nguyên tắc về tính thẳng thắn và sự hợp pháp

Thông tin về các cá nhân không thể được thu thập hay xử lý bằng những biện pháp không lành mạnh hay trái pháp luật, hay bị sử dụng cho những mục đích đi ngược với nguyên tắc và mục tiêu của Hiến chương Liên hợp quốc.

2. Nguyên tắc về sự đúng đắn, chính xác

Cá nhân chịu trách nhiệm đối với việc biên soạn các tệp tin hay trách nhiệm đối với việc thực hiện kiểm tra định kỳ về sự thích hợp, đúng đắn của dữ liệu được ghi chép, đồng thời đảm bảo rằng chúng hoàn toàn có khả năng tránh các lỗi sai sót, và chúng được cập nhật một cách thường xuyên hoặc khi thông tin chứa đựng trong một tệp tin được sử dụng, hoặc được xử lý.

3. Nguyên tắc của việc xác định mục đích

Mục đích mà một tệp tin đáp ứng cũng như những tiện ích của nó cần được định rõ, hợp pháp hóa và khi nó được tạo ra sẽ nhận được một lượng quan tâm nhất định từ công chúng hoặc mang lại sự chú ý của những người liên quan, nhằm sau đó tạo cho nó khả năng đảm bảo rằng:

a. Tất cả dữ liệu cá nhân được thu thập và ghi chép vẫn đầy đủ và phù hợp với mục đích đề ra;

b. Không có dữ liệu cá nhân nào nói trên được sử dụng hoặc tiết lộ cho những mục đích không phù hợp với quy định, ngoại trừ có sự đồng ý của người có liên quan; và

c. Giai đoạn mà dữ liệu cá nhân được lưu trữ không vượt quá khoảng thời gian cho phép đạt được những mục đích đã vạch ra.

4. Nguyên tắc truy cập của người quan tâm

Tất cả những ai cung cấp bằng chứng nhận dạng đều có quyền biết thông tin liên quan đến người đó có được xử lý và sử dụng dưới một hình thức minh bạch mà không chịu phí tổn hay chậm chễ quá mức hay không, đồng thời có sự chỉnh sửa hay xóa bỏ trong trường hợp thông tin đó không đúng, không cần thiết hay trái pháp luật, và khi nó được truyền đi thì có sự thông báo tới đối tượng đó.

5. Nguyên tắc không phân biệt đối xử

Tùy theo các trường hợp ngoại lệ giới hạn được nêu ra ở nguyên tắc 6, dữ liệu có khả năng bị cho là trái pháp luật hoặc phân biệt đối xử một cách tùy ý, bao gồm những thông tin về nguồn gốc dân tộc, màu da, giới tính, quan điểm chính trị, tư tưởng, tôn giáo và các tín ngưỡng khác cũng như là thành viên trong một hiệp hội hay nghiệp đoàn, không nên bị biên soạn.

6. Quyền tạo ra các trường hợp ngoại lệ

Xuất phát từ các nguyên tắc 1 đến 4 có thể chỉ được ủy quyền nếu chúng là cần thiết để bảo vệ an ninh quốc gia, trật tự công cộng, đạo đức hay sức khỏe cộng đồng, cũng như quyền tự do và các quyền của người khác, đặc biệt là những người đang bị bức hại (điều khoản nhân đạo), được xác định một cách rõ ràng trong luật hoặc quy tắc tương đương, ban hành theo quy định của hệ thống pháp luật nội bộ mà các quốc gia có những giới hạn và biện pháp bảo vệ phù hợp riêng của họ.

Ngoại lệ đối với nguyên tắc 5 có liên quan tới luật cấm phân biệt đối xử, ngoài những biện pháp bảo vệ tương tự như quy định ngoại lệ đối với các nguyên tắc 1 và 4, có thể được ủy quyền chỉ trong giới hạn được quy định bởi Luật quốc tế về Nhân quyền (International Bill of Human Rights) và những quy định có liên quan khác trong lĩnh vực bảo vệ nhân quyền và chống phân biệt đối xử.

7. Nguyên tắc an ninh

Những biện pháp thích hợp cần được thực thi nhằm bảo vệ các tiệp tin chống lại cả nguy cơ tự nhiên như sự phá hủy hay mất dữ liệu ngẫu nhiên, và nguy cơ do con người như truy cập trái phép, lạm dụng lừa đảo đối với dữ liệu hoặc sự lây nhiễm bởi virus máy tính.

8. Giám sát và trừng phạt

Luật pháp của mỗi quốc gia sẽ chỉ rõ quyền hạn, trách nhiệm đối với việc giám sát tuân theo các nguyên tắc, phù hợp với hệ thống pháp lý nội bộ từng nước. Quyền này sẽ tạo cơ hội cho việc đảm bảo tính công bằng, độc lập đối với những người hay tổ chức có trách nhiệm trong việc xử lý và lập dữ liệu, cũng như năng lực về mặt kỹ thuật. Trong trường hợp vi phạm các điều khoản về nguyên tắc thực thi luật quốc gia nói trên, các hình phạt sẽ được đưa ra cùng với những biện pháp khắc phục thích hợp.

9. Trao đổi dữ liệu

Khi pháp luật của hai hai nhiều quốc gia liên quan tới việc trao đổi dữ liệu xuyên biên giới đưa ra các biện pháp về đảm bảo bí mật riêng tư, thông tin sẽ có thể lưu thông một cách tự do bên trong mỗi vùng lãnh thổ có liên quan. Nếu không có biện pháp bảo vệ lẫn nhau, việc giới hạn lưu thông có thể không được áp đặt để bảo đảm các nhu cầu bí mật riêng tư.

10. Lĩnh vực ứng dụng

Những nguyên tắc hiện tại cần tạo ra khả năng áp dụng đối với tất cả các tệp tin được lưu trữ trong máy tính công cộng và cá nhân bằng các biện pháp mở rộng tùy chọn và theo hướng điều chỉnh phù hợp. Một số quy định đặc biệt, cũng có thể tùy chọn, có thể được thực hiện giúp mở rộng tất cả hay một phần các nguyên tắc đối với những tệp tin của các cá nhân hợp pháp, đặc biệt là khi chúng chứa đựng một số thông tin về cá nhân.[46]

Chỉ thị về bảo vệ dữ liệu của EU

Ngày 24/10/1995, Hội đồng Bộ trưởng EU đã thông qua Chỉ thị Châu Âu về Bảo vệ dữ liệu cá nhân (European Directive on the Protection of Individuals) với Chỉ thị về Xử lý dữ liệu cá nhân (Regard to Processing of Personal Data) và Tự do di chuyển dữ liệu (Free Movement of Such Data), còn gọi là Chỉ thị EU, nhằm đưa ra một khung điều tiết đảm bảo cho việc di chuyển dữ liệu cá nhân an toàn và tự do trong khối các quốc gia thành viên EU, thêm vào đó, thiết lập một ranh giới an ninh xung quan dữ liệu cá nhân ở bất kỳ nơi nào nó được lưu trữ, truyền tải và xử lý.

Chỉ thị Bảo vệ dữ liệu EU được xây dựng trong một nỗ lực nhằm thống nhất và hài hòa các luật lệ riêng của từng nước có liên quan đến vấn đề bảo vệ bí mật riêng tư. Điều khoản 1 của Chỉ thị EU quy định rằng "Các chính phủ thành viên sẽ bảo vệ các quyền cơ bản và quyền tự do của thể nhân, và đặc biệt là quyền bí mật riêng tư của họ, với sự tôn trọng đối với việc xử lý dữ liệu cá nhân."

Chỉ thị EU cấm việc chuyển giao thông tin cá nhân cho các quốc gia không có mức độ bảo vệ đầy đủ, dẫn tới sự đối lập giữa EU và chính phủ Mỹ.[47]

Mỗi quốc gia thành viên EU đều đã xem xét lại bộ luật hiện tại của mình hoặc xây dựng một bộ luật về bảo vệ bí mật riêng tư mới để thực hiện Chỉ thị EU.

Các ví dụ khác trong luật pháp EU về bảo vệ bí mật riêng tư như Điều khoản 8 của Công ước Châu Âu về Nhân quyền (European Convention on Human Rights), Chỉ thị 95/46/EC (Chỉ thị về Bảo vệ dữ liệu), Chỉ thị 2002/58/EC (Chỉ thị E-Privacy), và Điều khoản 5 của Chỉ thị 2006/24/EC (Chỉ thị về Lưu trữ dữ liệu).[48]

---

[46] Các nguyên tắc được trích từ Văn phòng Cao ủy về nhân quyền (Office of the High Commissioner for Human Rights), "Guidelines for the Regulation of Computerized Personal Data Files," http://www.unhchr.ch/html/menu3/b/71.htm.

[47] Domingo R. Tan, Comment, Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union, 21 LOY. L.A. INT'L & COMP. L.J. 661, 666 (1999).

[48] Justice and Home Affairs, "Data Protection," European Commission, http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm.

Quy định bảo vệ bí mật riêng tư của Hàn Quốc

Hàn Quốc là quốc gia có số lượng thuê bao băng rộng lớn nhất thế giới. Tính đến nửa đầu 2005, 25% dân số và 75% số hộ gia đình đã đăng ký sử dụng mạng băng rộng.[49] Hiện nay, mạng băng rộng và mạng truyền thông vô tuyến của Hàn Quốc được biết đến là một trong những hệ thống tốt nhất thế giới. Theo đó, tần suất của sự rò rỉ thông tin cá nhân trong nước cũng tăng lên đáng kể, và cần một giải pháp cả về công nghệ lẫn chính sách.

Tuy nhiên, Chính phủ Hàn Quốc lại không hành động đủ nhanh để đối mặt với vấn đề này. Luật Bảo vệ Bí mật riêng tư (Privacy Prôtectin Law) vẫn đang chờ Quốc hội giải quyết và chưa có bộ luật độc lập nào cho vấn đề bảo vệ thông tin cá nhân.

Mặt khác, Chính phủ Hàn Quốc đã xây dựng "Lộ trình An ninh Thông tin trung và dài hạn cho việc hiện thực hóa u-SafeKorea" (Mid and Long-term Information Security Roadmap for Realizing u-SafeKorea) và bốn dự án ưu tiên hàng đầu kể từ 2005 trong đó là: (1) bảo đảm an toàn cho cơ sở hạ tầng tiên tiến; (2) gây dựng niềm tin đối với các dịch vụ IT mới; (3) tăng cường các chức năng bảo vệ thông tin cho các động cơ tăng trưởng mởi; và (4) xây dựng một cơ sở an ninh thông tin trong một môi trường mạng mới. Bố ưu tiên này có bao gồm một dự án con được gọi tên là "Tăng cường Hệ thống Bảo vệ Bí mật riêng tư" (Strengthening Privacy Protection System).

Hơn nữa, đã có một số bộ luật có liên quan tới vấn đề bảo vệ bí mật riêng tư như "Luật Bảo vệ Thông tin Cá nhân tại nơi công cộng" (Personal Information Protection Law in Public) và "Luật Bảo vệ Thông tin và Mạng lưới Viễn thông" (Law on Telecom Networks and Information Protection).

Luật Bảo vệ Thông tin Cá nhân tại nơi công cộng: Bộ luật này bao gồm các quy định về bảo vệ bí mật riêng tư đối với việc nắm giữ và quản lý thông tin cá nhân được xử lý trong máy tính tại các cơ quan công cộng, cũng như các quy định có liên quan tới hiệu quả hợp lý của các nhiệm vụ công, và bảo vệ quyền và lợi ích của con người.

Đạo luật Thúc đẩy Bảo vệ thông tin và Sử dụng mạng lưới thông tin và truyền thông (Act on Promotion of Information and Communication Network Utilization and Information Protection): Mục tiêu của Đạo luật là nhằm cải tiến hệ thống bảo vệ bí mật riêng tư trong khối tư nhân, theo sự mở rộng của mạng truyền thông thông tin và sự suy rộng việc thu thập cũng như phân phối thông tin cá nhân. Đạo luật tuân theo quy trình bảo vệ bí mật riêng tư dựa trên vòng đời của thông tin cá nhân như chu trình thu thập, sử dụng, quản lý và xóa bỏ. Đạo luật cũng bao gồm các quy định liên quan tới các quyền của người sử dụng thông tin cá nhân cũng như việc thiết lập và điều hàn một ủy ban dàn xếp các vấn đề bí mật riêng tư.

[49] Internet World Stats, "Korea," Miniwatts Marketing Group, http://www.internetworldstats.com/asia/kr.htm.

Đạo luật Bảo vệ Bí mật liên lạc (Protection of Communication Secrets Act): Đạo luật giới hạn phạm vi mục tiêu của bí mật riêng tư và tự do liên lạc nhằm bảo vệ bí mật liên lạc cũng như đảm bảo quyền tự do về liên lạc. Luật không cho phép sự xâm phạm bí mật đàm thoại như thông qua hình thức ghi âm hay nghe trộm, đồng thời nó cũng bảo vệ các bí mật trong liên lạc.

Đạo luật Bảo vệ Thông tin về vị trí (Location Information Protection Act): Đạo luật hướng tới điều tiết việc thu thập và sử dụng thông tin về vị trí nhằm bảo vệ chống lại sự rò rỉ, lạm dụng/sử dụng sai mục đích đối với thông tin; đồng thời khuyến khích sử dụng thông tin trong một môi trường an toàn. Đạo luật công nhận khả năng của công nghệ truyền thông ngày nay trong việc xác định vị trí của một cá nhân (ví dụ thông qua điện thoại di động), và thực tế là sự rò rỉ về thông tin vị trí có thể gây ra những hành vi xâm phạm bí mật riêng tư nghiêm trọng. Do đó, luật tạo ra những quy tắc không bao giờ tiết lộ thông tin về vị trí trừ trường hợp pháp luật yêu cầu.

Bảo vệ bí mật riêng tư tại Mỹ

Mỹ đã giao phó hoạt động bảo vệ bí mật riêng tư cho thị trường kể từ khi quá nhiều hạn chế của chính phủ đã cản trở các hoạt động thương mại điện tử. Kết quả là các chứng thực bí mật riêng tư như Trust-e hay Better Business Bureau Online đã nổi lên, và pháp luật về bảo vệ bí mật riêng tư đã không được tích hợp vào. Luật Bí mật riêng tư 1974 quy định đối với việc bảo vệ bí mật riêng tư về thông tin trong khu vực công trong khi những luật pháp khác thì chi phối bí mật riêng tư trong khu vực tư. Chưa có tổ chức nào đề cập đến tất cả các vấn đề bảo vệ bí mật riêng tư trong khu vực tư. Trong khu vực công, Cục Quản lý hành chính và Ngân sách (Office of Management and Budget - OMB) đảm nhận vai trò xây dựng chính sách bí mật riêng tư của chính quyền liên bang dựa theo Luật Bí mật riêng tư (Privacy Law). Trong khu vực tư, Ủy ban Thương mại Liên bang (Federal Trade Commission) được ủy quyền thực thi pháp luật bảo vệ bí mật riêng tư trực tuyến của trẻ em, thông tin tín dụng của khách hàng và thực tiễn hoạt động thương mại.

Các luật pháp của Mỹ liên quan tới bảo vệ bí mật riêng tư bao gồm:

- Luật Bí mật riêng tư (Privacy Act), 1974
- Luật Bảo vệ Tính dụng Khách hàng (Consumer Credit Protection Act), 1984
- Luật Bí mật riêng tư trong Liên lạc điện tử (Electric Communications Privacy Act), 1986
- Luật Gramm-Leach-Bliley (Gramm-Leach-Bliley Act), 1999
- Luật Trách Lợi Bảo hiểm Y tế (Health Insurance Portability and Accountability Act), 1996

. Luật Sarbanes-Oxley (Sarbanes-Oxley Act), 2002

. Luật Bảo vệ Bí mật riêng tư trực tuyến của trẻ em (Children's Online Privacy Protection Act), 1998

Các biện pháp bảo vệ bí mật riêng tư của Nhật Bản

Năm 1982, Nhật Bản xây dựng một biện pháp bảo vệ bí mật riêng tư dựa trên 8 nguyên tắc cơ bản của OECD. Năm 1998, bộ luật về bảo vệ bí mật riêng tư trong khu vực công đã được ban hành và có hiệu lực. Trong lĩnh vực tư, Hướng dẫn về Bảo vệ bí mật riêng tư (Guideline for the Protection of Privacy) đã được ban hành năm 1997 bởi Bộ Công nghiệp và Thương mại quốc tế (Ministry of International Trade and Industry). Nhằm thúc đẩy sự tuân thủ đối với các bộ luật bảo vệ bí mật riêng tư quốc gia với những hướng dẫn quốc tế, Trụ sở Khuyến khích xã hội về Viễn thông và Thông tin nâng cao (Advanced Information and Telecommunications Society Promotion Headquarters) đã đưa ra pháp luật về bảo vệ bí mật thông tin cá nhân.

Ngoài ra, Cơ quan Bảo vệ Dữ liệu (Data Protection Authority) được chỉ định như một đơn vị độc lập đảm bảo tuân thủ đúng các quy định bảo vệ bí mật riêng tư và hỗ trợ các cá nhân trong trường hợp bị xâm phạm bí mật riêng tư. Cơ quan Bảo vệ Dữ liệu được ủy quyền để cải thiện tính minh bạch trong xử lý thông tin đảm bảo các quyền và lợi ích của đối tượng sở hữu dữ liệu, và bảo đảm rằng các đơn vị xử lý thông tin cũng như những người sử dụng thông tin thực hiện đầy đủ trách nhiệm của mình. Cơ quan này cũng được mong đợi sẽ đóng vai trò trong việc bảo vệ lợi ích quốc gia, đặc biệt là trong các trường hợp truyền tải thông tin xuyên quốc gia.

Các bộ luật của Nhật Bản liên quan đên bảo vệ bí mật riêng tư bao gồm:

. Luật Bảo vệ Dữ liệu cá nhân được xử lý bởi máy tính trong Cơ quan hành chính (Act for the Protection of Computer Processed Personal Data Held by Administrative Organs), 1988

. Quy chế của các Chính quyền địa phương (Regulations of Local Governments) (được ban hành năm 1999 cho 1,529 chính quyền địa phương)

. Luật Bảo vệ Thông tin Cá nhân (Act for the Protection of Personal Information), 2003

. Luật Bảo vệ Thông tin Cá nhân trong các Cơ quan hành chính (Act on the Protection of Personal Information Held by Administrative Organs), 2003

. Luật Bảo vệ Thông tin Cá nhân được lưu trữ bởi các Đơn vị hành chính độc lập (Act for the Protection of Personal Information Retained by Independent Administrative Institutions), 2003

. Bộ luật Kiểm toán (Board of Audit Law), 2003

. Hướng dẫn Bảo vệ Bí mật riêng tư có liên quang tới thẻ RFID (Guidelines for Privacy Protection with regard to RFID Tags), 2004

Câu hỏi suy nghĩ

1. Tại đất nước bạn, những bộ luật và chính sách nào được áp dụng để bảo vệ bí mật riêng tư về thông tin?
2. Những vấn đề hay sự cân nhắc nào tác động đến việc ban hành và/hoặc thực thi luật và chính sách?
3. Những nguyên tắc nào (trong Hướng dẫn của OECD và Hướng dẫn của UN) bạn cho là nền tảng của các luật và chính sách liên quan đến bảo vệ bí mật riêng tư ở đất nước bạn?

5.3. Đánh giá tác động bí mật riêng tư (Privacy Impact Assessment - PIA)

PIA là gì?

PIA là một quá trình có hệ thống của việc nghiên cứu, phân tích và đánh giá tác động tới bí mật riêng tư của các quốc gia hay khách hàng về việc đưa ra những hệ thống thông tin mới hoặc chỉnh sửa những hệ thống thông tin hiện có. PIA được dựa trên 'nguyên tắc phòng chống sơ bộ' (principle of preliminary prevention) – nghĩa là phòng bệnh hơn là chữa bệnh. Nó không chỉ đơn giản là một hệ thống đánh giá mà còn xem xét những tác động quan trọng tới bí mật riêng tư đối với việc đưa ra hay thay đổi những hệ thống mới. Do vậy, nó khác với kiểm tra việc bảo vệ bí mật riêng tư ở chỗ đảm bảo sự thực thi những yêu cầu bên ngoài và chính sách nội bộ đối với bí mật riêng tư.

Do PIA được chỉ đạo để phân tích khía cạnh xâm phạm bí mật riêng tư khi một hệ thống mới được xây dựng, nó không cần phải tiến hành ở giai đoạn đầu của sự phát triển, khi mà những thay đổi đối với các đặc điểm phát triển vẫn có thể xảy ra. Tuy nhiên, khi một nguy cơ xâm phạm nghiêm trọng tìm thấy trong quá trình thu thập, sử dụng và quản lý thông tin cá nhân trong lúc vận hành các dịch vụ đã có, sẽ là cần thiết để tiến hành một PIA và sau đó điều chỉnh hệ thống hiện tại.

Quy trình PIA[50]

Thông thường, một PIA bao gồm 3 bước (Bảng 10).

Bảng 10. Quy trình PIA

[50] Được trích tại Privacy Office, Privacy Impact Assessment: A User's Guide (Ontario: Management Board Secretariat, 2001), http://www.accessandprivacy.gov.on.ca/english/pia/pia1.pdf.

Phân tích mặt khái niệm (Conceptual Analysis)	Phân tích luồng dữ liệu (Data Flow Analysis)	Phân tích tiếp theo (Follow-up Analysis)
Chuẩn bị một bản mô tả đơn giản về phạm vi tính hợp lý của các sáng kiến được đề xuất Xác định trong một cách thức sơ bộ về các vấn đề bí mật riêng tư tiềm năng cũng như các mối rủi ro và những đối tượng liên quan chính Đưa ra một bản mô tả chi tiết về những khía cạnh thiết yếu của đề xuất, bao gồm phân tích chính sách của những vấn đề chính Xây dựng tài liệu về các luồng thông tin cá nhân chủ đạo Xây dựng bản nghiên cứu các vấn đề môi trường nhằm xem xét xem liệu có đối tượng nào khác cũng nghiên cứu một sáng kiến tương tự Xác định các đối tượng liên quan và quan tâm Đánh giá phản ứng của công chúng	Phân tích các luồng dữ liệu thông qua biểu đồ quy trình hoạt động và xác định những yếu tố dữ liệu hay nhóm dữ liệu cá nhân cụ thể Đánh giá sự tuân thủ quyền tự do thông tin (Freedom of Information - FOI) và pháp luật về bí mật riêng tư cũng như các quy chế có liên quan của đề xuất. Đánh giá sự phù hợp của đề xuất đối với những nguyên tắc chung về bí mật riêng tư Tiến hành phân tích rủi ro dựa trên phân tích sáng kiến và xác định các giải pháp có thể Xem xét lại các tùy chọn thiết kế và xác định các vấn đề liên quan đến bí mật riêng tư mà chưa được xử lý Chuẩn bị một giải pháp cho những vấn đề về bí mật riêng tư chưa được giải quyết	Xem xét lại và phân tích thiết kế hệ thống và phần cứng vật lý trong sáng kiến đề xuất nhằm đảm bảo phù hợp với những yêu cầu thiết kế đối với bí mật riêng tư Đưa ra bản xem xét cuối cùng về sáng kiến được đề xuất Kiểm tra phân tích rủi ro và bí mật riêng tư của bất kỳ thay đổi mới nào đối với sáng kiến đề xuất có liên quan đến thiết kế phần mềm và phần cứng nhằm đảm bảo phù hợp với FOI và pháp luật về bí mật riêng tư, các quy chế có liên quan cũng như các nguyên tắc chung về bí mật riêng tư Chuẩn bị một kế hoạch truyền thông

Nguồn: Information and Privacy Office, Privacy Impact Assessment: A User's Guide (Ontario: Management Board Secretariat, 2001), 5, http://www.accessandprivacy.gov.on.ca/english/pia/pia1.pdf.

Đánh giá phạm vi của PIA

Một PIA được thực hiện khi:

Xây dựng một hệ thống thông tin mới mà nó sẽ nắm giữ và quản lý một số lượng lớn về thông tin cá nhân;

Sử dụng một kỹ thuật mới tại nơi mà bí mật riêng tư có thể bị xâm phạm;

Sửa đổi hệ thống thông tin hiện có đang nắm giữ và quản lý thông tin cá nhân; và

Thu thập, sử dụng, duy trì và/hoặc hủy thông tin cá nhân trong suốt quá trình mà một rủi ro về xâm phạm bí mật riêng tư có thể xảy ra.

Tuy nhiên, không cần thiết thực thi một PIA trên toàn bộ các hệ thống hiện có. Một PIA không cần phải tiến hành khi chỉ có một thay đổi nhỏ trong chương trình và hệ thống hiện tại.

Ví dụ về các PIA

Bảng 11 liệt kê các hệ thống PIA tai 3 quốc gia Mỹ, Canada, Úc

Bảng 11. Các ví dụ về PIA

	Mỹ	Canada	Úc/New Zealand
Nền tảng luật pháp	Mục 208 của Luật Chính phủ điện tử (e-Government) năm 2002 OMB đưa ra các yêu cầu PIA trong OMB-M-03-22	Giới thiệu chính sách và hướng dẫn PIA của mình vào tháng 5/2002 Bắt buộc thực hiện PIA trên cơ sở chính sách và luật pháp chung	Tự nguyện tiến hành PIA (không có cơ sở pháp lý) PIA Handbook hỗ trợ cho PIA (2004, New Zealand), hướng dẫn PIA (2004, Úc)
Chủ thể	Tất cả các cơ quan và ban ngành hành pháp cũng như nhà thầu sử dụng IT hay các đơn vị vận hành website cho mục đích tương tác với công chúng; Các sáng kiến liên ngành có liên quan, bao gồm cả những sáng kiến đẩy mạnh chính phủ điện tử	Tất cả những dịch vụ và chương trình mà các cơ quan chính phủ cung cấp	Không quy định trách nhiệm hay giới hạn

Đối tượng	Các cơ quan thực thi dự án chính phủ điện tử có giao dịch với thông tin cá nhân	Những cơ quan chính phủ phát triển hay vận hành các dịch vụ và chương trình	Những cơ quan có liên quan hoặc yêu cầu đơn vị tư vấn bên ngoài
Sự công bố	Xây dựng PIA công khai và sẵn sàng cung cấp qua website của đơn vị, công bố tại Cơ quan Đăng ký Liên bang, hoặc những biện pháp khác có thể bị thay đổi hay khước từ vì các lý do an ninh hoặc để bảo vệ thông tin cá nhân bí mật, nhạy cảm có trong đánh giá Các cơ quan sẽ cung cấp cho Cục OMB (Director of OMB) một bản sao của PIA cho mỗi hệ thống được yêu cầu	Xây dựng PIA tổng hợp công khai và sẵn sàng cung cấp Cung cấp một bản sao của PIA cuối cùng và báo cáo với Văn phòng Hội đồng Bí mật riêng tư (Office of the Privacy Commissioner) nhằm nhận được chỉ dẫn và lời khuyên đúng đắn đối với các khía cạnh trong chiến lược bảo vệ	Kết quả của PIA thường không được công bố công khai (không quy định trách nhiệm báo cáo và công bố)

Tự kiểm tra

1. Thông tin cá nhân thì khác gì so với những loại thông tin khác?
2. Tại sao thông tin cá nhân cần được bảo vệ?
3. Đâu là sự cần thiết đối với các nguyên tắc của OECD và UN về bảo vệ bí mật riêng tư?
4. Tại sao phải tiến hành đánh giá tác động bí mật riêng tư?

6. SỰ THÀNH LẬP VÀ HOẠT ĐỘNG CỦA CSIRT

Phần này nhằm mục đích:

. Giải thích làm thế nào để xây dựng và vận hành Nhóm ứng cứ sự cố an toàn máy tính (Computer Security Incident Response Team - CSIRT); và

. Đưa ra các mô hình CSIRT từ nhiều quốc gia khác nhau.

Tội phạm mạng và nhiều mối đe dọa đối với an ninh thông tin cần được nắm bắt một cách nghiêm túc bởi tác động to lớn về mặt kinh tế của chúng. Ví dụ, Hiệp hội An ninh mạng Nhật Bản (Japan Network Security Association) ước tính trong năm 2006, thiệt hại kinh tế từ sự thất thoát thông tin cá nhân 446 triệu USD – tương đương 347USD mỗi người. Ferris Research dự tính thiệt hại do thư rác tại Mỹ đã lên tới xấp xỉ 8.9 tỉ USD trong năm 2002, 20 tỉ USD trong năm 2004 và 50 tỉ USD trong năm 2005.

Việc thiết lập CSIRT là một biện pháp hiệu quả giúp giảm nhẹ và giảm thiểu thiệt hại từ những cuộc tấn công vào các hệ thống thông tin và sự vi phạm an ninh thông tin.

6.1. Phát triển và vận hành một CSIRT

CSIRT là một tổ chức, được chính thức hóa hay vì mục đích đảm nhiệm việc tiếp nhận, xem xét lại và đáp lại những hoạt động cũng như các báo cáo sự cố an ninh máy tính. Mục đích cơ bản của một CSIRT là cung cấp các dịch vụ quản lý sự cố an ninh máy tính nhằm giảm thiểu thiệt hại và cho phép khôi phục hiệu quả từ một sự cố an ninh máy tính.[51]

Năm 1998, sự bùng nổ lần đầu tiên của một sâu máy tính có tên Morris đã xảy ra và lan rộng một cách nhanh chóng trên toàn thế giới. Sau đó, Cơ quan phụ trách các dự án nghiên cứu cao cấp về quốc phòng (Defence Advanced Research Projects Agency) đã sáng lập ra Viện Kỹ sư Phần mềm (Software Engineering Institute) và tiếp đó đã thành lập CERT/CC tại Trường đại học Carnegie Mellon theo hợp đồng của Chính phủ Hoa Kỳ. Kể từ đó, mỗi quốc gia Châu Âu đã thành lập một tổ chức tương tự. Khi mà không có CSIRT đơn độc nào có thể giải quyết các sự cố tấn công rộng rãi, Diễn đàn của các Nhóm An ninh và Ứng cứ sự cố (Forum of Incident Response and Security Teams – FIRST) được thành lập năm 1990. Thông qua FIRST, nhiều cơ quan an ninh thông tin và CSIRT có thể trao đổi ý kiến và chia sẻ thông tin với nhau.

[51] CERT, "CSIRT FAQ," Carnegie Mellon University, http://www.cert.org/csirts/csirt_faq.html.

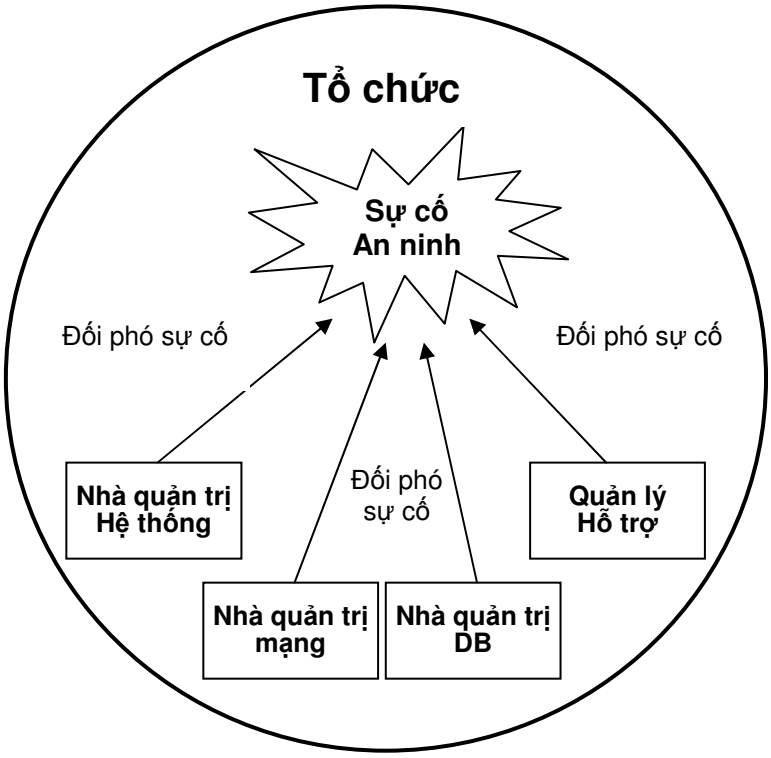
Lựa chọn đúng mô hình CSIRT[52]

Có 5 mô hình tổ chức chung cho CSIRT. Mô hình phù hợp nhất đối với một tổ chức – có nghĩa là tính toán đến rất nhiều điều kiện như môi trường, hiện trạng tài chính và nguồn nhân lực – cần được thông qua.

1. Mô hình Nhóm an ninh (sử dụng đội ngũ IT hiện có)

Mô hình nhóm an ninh không phải là một mô hình CSIRT chuẩn. Trên thực tế, nó đối lập với mô hình CSIRT chuẩn. Trong mô hình này, không có tổ chức mang tính tập trung được trao trách nhiệm quản lý các sự cố an ninh máy tính. Thay vào đó, các nhiệm vụ quản lý sự cố được chỉ đạo bởi những nhà quản trị mạng và hệ thống, hoặc bởi những chuyên gia hệ thống an ninh khác.

Hình 14. Mô hình nhóm an ninh



2. Mô hình CSIRT phân tán bên trong

Mô hình này cũng có thể hiểu là 'CSIRT phân tán' (distributed CSIRT). Nhóm trong mô hình này bao gồm nhà quản trị CSIRT, người có trách nhiệm báo quản lý tổng thể và báo cáo, và đội ngũ nhân viên từ các phòng ban khác của doanh nghiệp/ cơ quan có liên quan. CSIRT trong mô hình này là một tổ chức được công nhận một cách chính thức với nhiệm vụ quản lý toàn bộ các

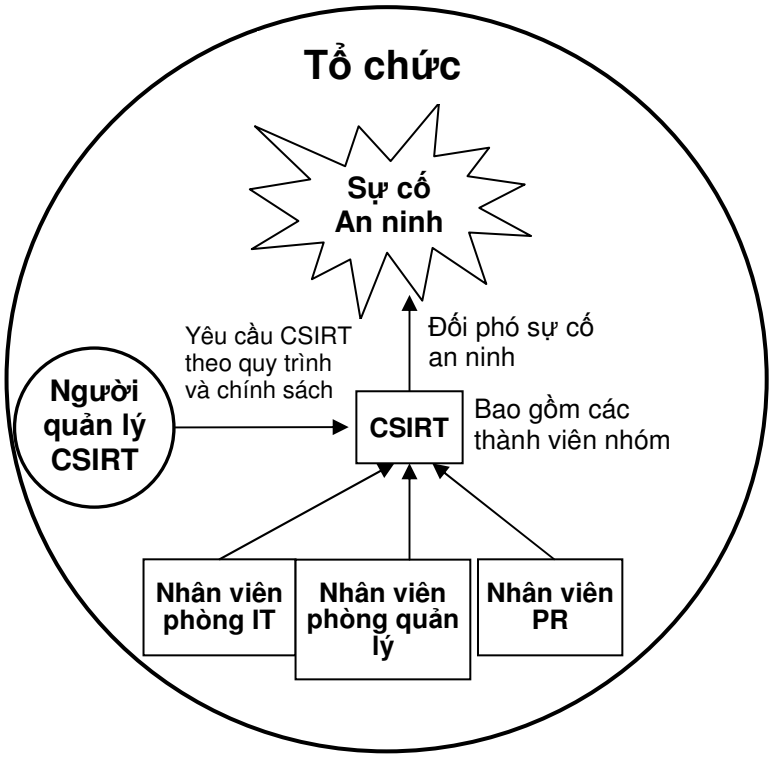
[52] Được trích tại Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle and Mark Zajicek, Organizational Models for Computer Security Incident Response Teams (CSIRTs) (Pittsburgh: Carnegie Mellon University, 2003), http://www.cert.org/archive/pdf/03hb001.pdf.

hoạt động đối phó sự cố. Vì nhóm được xây dựng bên trong một công ty hay một cơ quan nên nhóm được coi là 'nội bộ'.

Mô hình CSIRT phân tán nội bộ khác với mô hình nhóm an ninh ở những điểm sau:

- Các chính sách, thủ tục và quy trình quản lý sự cố được chính thức hóa nhiều hơn;
- Phương pháp truyền thông được thiết lập với toàn bộ doanh nghiệp có liên quan đến các mối đe dọa về an ninh và những chiến lược đối phó; và
- Người quản lý CSIRT và các thành viên nhóm được chỉ định là những người được phân công cụ thể những nhiệm vụ quản lý sự cố.

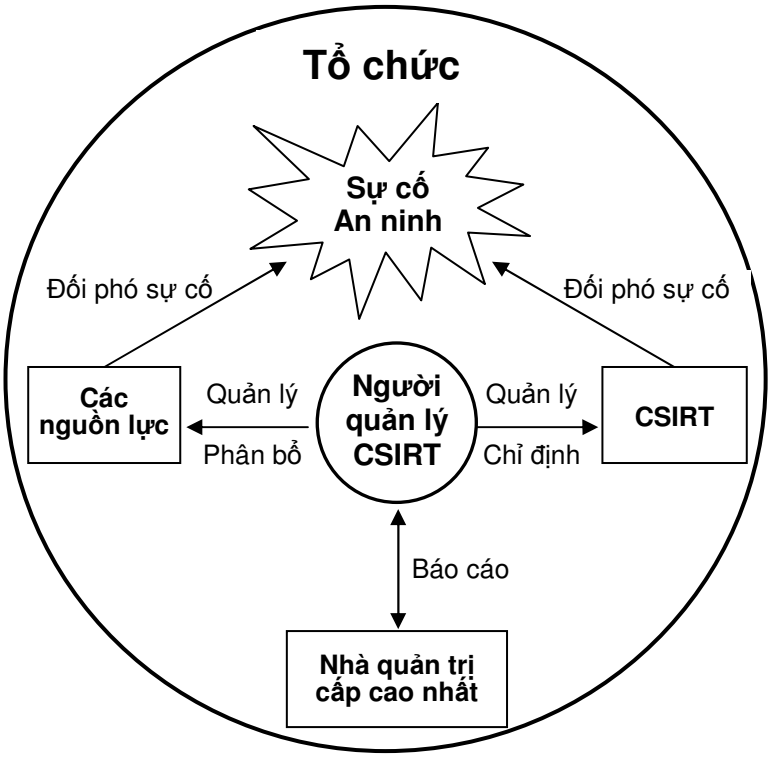
Hình 15. Mô hình CSIRT phân tán nội bộ



3. Mô hình CSIRT tập trung nội bộ

Trong mô hình CSIRT tập trung nội bộ, một nhóm được đặt ở trung tâm sẽ điều khiển và hỗ trợ tổ chức. CSIRT chịu trách nhiệm tổng thể đối với việc báo cáo, phân tích và đối phó với toàn bộ các sự cố. Do đó các thành viên của nhóm không đảm nhiệm các công việc khác và dành toàn bộ thời gian làm việc của họ để hoạt động trong đội và kiểm soát tất cả những sự cố. Đồng thời, người quản lý CSIRT có trách nhiệm báo cáo với cấp quản lý cao hơn như Nhà quản trị Thông tin (Chief Information Officer), Nhà quản trị An ninh (Chief Security Officer) hay Nhà quản trị Rủi ro (Chief Risk Officer).

Hình 16. Mô hình CSIRT tập trung nội bộ

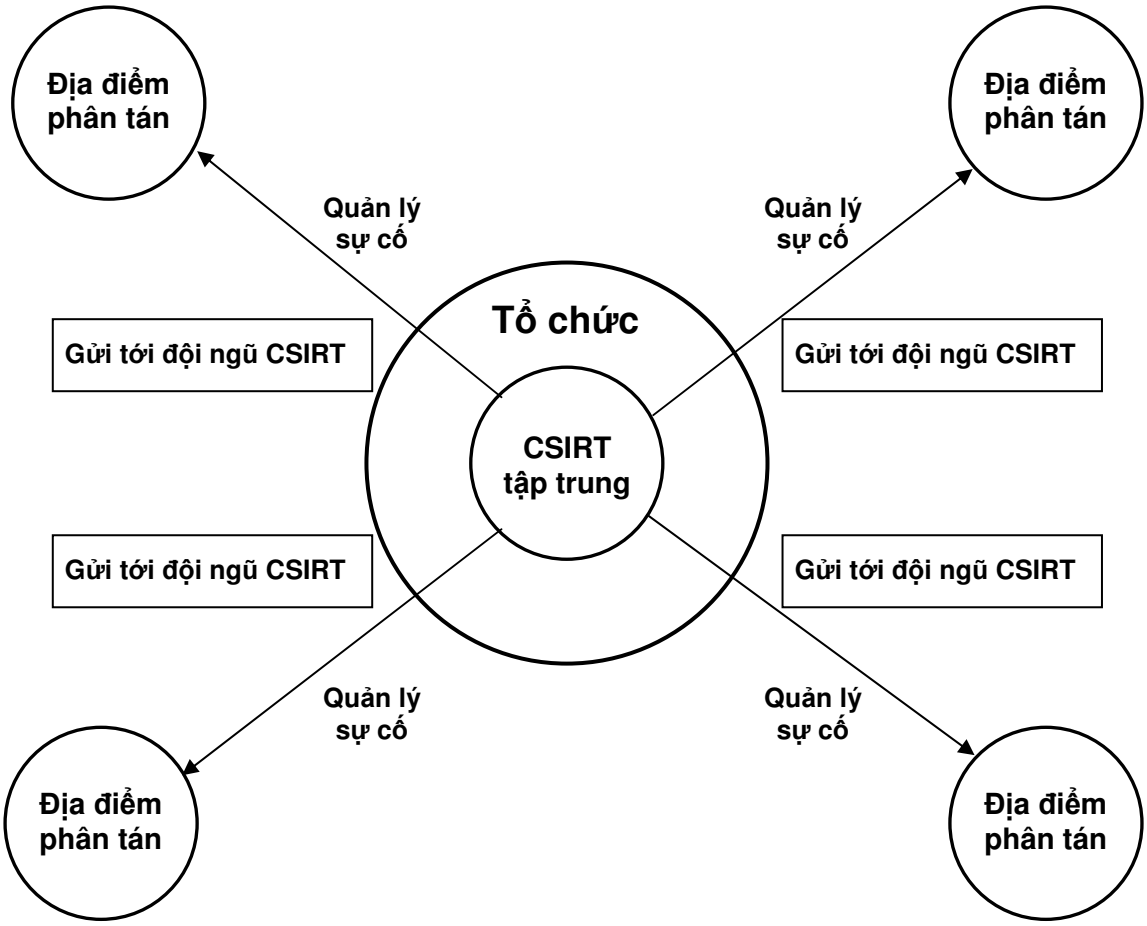


4. Mô hình CSIRT tập trung và phân tán kết hợp

Mô hình này cũng được biết đến là 'CSIRT kết hợp'. Nơi mà một CSIRT tập trung không thể kiểm soát và hỗ trợ cho toàn bộ tổ chức, những thành viên nhóm được phân tán ở các phòng ban/chi nhánh/địa điểm của tổ chức cung cấp trong phạm vi trách nhiệm của mình cùng một mức dịch vụ như được cung cấp bởi CSIRT tập trung.

Nhóm tập trung đưa ra các chiến lược giảm nhẹ và những biện pháp khôi phục, phân tích dữ liệu ở cấp cao. Nó cũng cung cấp cho các thành viên nhóm phân tán sự hỗ trợ đối phó nhất định đối với khả năng bị tấn công, sự cố. Các thành viên nhóm phân tán tại mỗi địa điểm sẽ thực thi các chiến lược và đưa ra ý kiến chuyên môn trong lĩnh vực của mình.

Hình 17. Mô hình CSIRT kết hợp



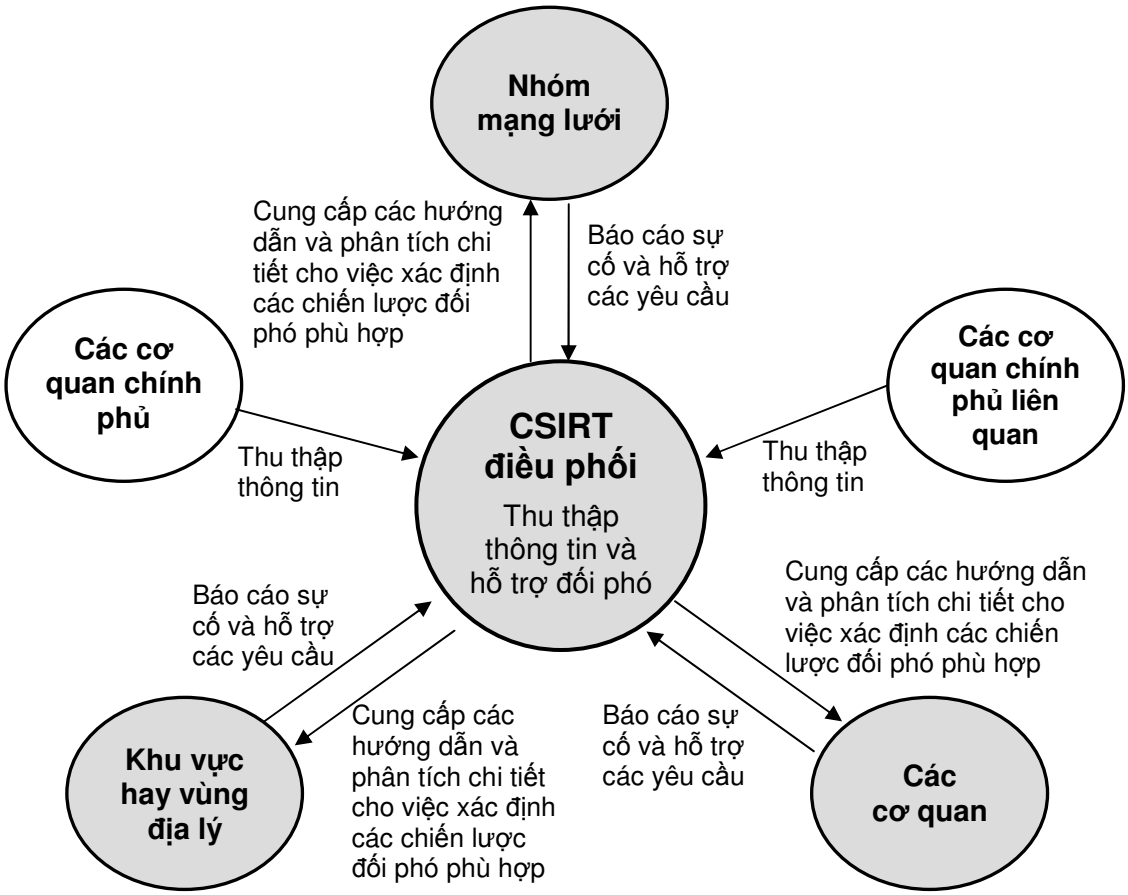
5. Mô hình CSIRT điều phối

Một mô hình CSIRT sẽ tăng cường chức năng của các nhóm phân tán trong mô hình CSIRT tập trung. Trong mô hình CSIRT điều phối, thành viên nhóm trong CSIRT kết hợp được gộp lại thành những CSIRT độc lập trên cơ sở các đặc điểm như kết nối mạng lưới, ranh giới địa lý… Tất cả được điều khiển bởi CSIRT trung tâm.

Mô hình CSIRT điều phối thì phù hợp với một hệ thống CSIRT quốc gia. Mô hình này có thể được áp dụng cho các hoạt động nội bộ trong một tổ chức đồng thời hỗ trợ và phối hợp chặt chẽ với các cơ quan bên ngoài.

Những hoạt động điều phối và tạo điều kiện thuận lợi bao gồm chia sẻ thông tin, cung cấp các chiến lược giảm nhẹ, phương pháp khôi phục, biện pháp đối phó sự cố, nghiên cứu/phân tích các xu hướng và hình mẫu của hoạt động đối phó sự cố, cơ sở dữ liệu các khả năng có thể bị tấn công, trung tâm xử lý cho các công cụ an ninh, và các dịch vụ cố vấn, cảnh báo.

Hình 18. Mô hình CSIRT điều phối



Thiết lập một CSIRT: Các bước để lập một CSIRT quốc gia[53]

Có 5 giai đoạn trong quá trình thiết lập một CSIRT. Mục tiêu, tầm nhìn và vai trò của CSIRT sẽ là chỉ dẫn trong quá trình thực hiện của toàn bộ các giai đoạn.

Giai đoạn 1 – Giáo dục các bên liên quan về sự phát triển của một nhóm trên phạm vi quốc gia

Giai đoạn 1 là giai đoạn nhận thức, nơi các bên liên quan phát triển sự hiểu biết về những gì có liên quan đến việc thiết lập CSIRT. Thông qua rất nhiều phương pháp giáo dục, họ có thể học hỏi được:

a. Động lực và động cơ kinh doanh đằng sau nhu cầu về một CSIRT quốc gia
b. Các yêu cầu đối với việc phát triển năng lực đối phó sự cố của một CSIRT quốc gia
c. Xác định những người có liên quan trong quá trình bàn bạc về việc xây dựng một nhóm trên phạm vi quốc gia

[53] Được trích tại Georgia Killcrece, Steps for Creating National CSIRTs (Pittsburgh: Carnegie Mellon University, 2004), http://www.cert.org/archive/pdf/NationalCSIRTs.pdf.

d. Các nguồn lực chính và cơ sở hạ tầng thiết yếu đã có của quốc gia
e. Các loại hình kênh truyền thông cần được xác định cho việc liên lạc với thành viên CSIRT
f. Các quy định, luật pháp cụ thể và những chính sách khác mà sẽ tác động tới sự phát triển của một CSIRT quốc gia
g. Các chiến lược tài trợ có thể được sử dụng để phát triển, hoạch định, thực thi và vận hành năng lực đối phó
h. Cơ sở hạ tầng thông tin mạng lưới và công nghệ mà sẽ cần thiết cho việc hỗ trợ hoạt động của nhóm quốc gia
i. Các kế hoạch đối phó cơ bản và tương hỗ được áp dụng trên nhiều lĩnh vực
j. Tập các dịch vụ cốt lõi tiềm năng mà một CSIRT quốc gia có thể cung cấp cho các thành viên của mình
k. Các hướng dẫn và bài học thực tiễn tốt nhất

Giai đoạn 2 – Hoạch đinh CSIRT: Kết nối các thông tin và kiến thức có được trong giai đoạn 1

Giai đoạn 2 liên quan tới việc hoạch định CSIRT dựa trên thông tin và kiến thức thu được trong suốt giai đoạn 1. Những vấn đề được thảo luận trong giai đoạn 1 được xem xét lại và thảo luận sâu hơn, và sau đó những chi tiết cụ thể được xác định và đưa vào bản kế hoạch thực thi. Bản kế hoạch được xây dựng có tính toán đến các hoạt động sau:

a. Nhận diện những yêu cầu và nhu cầu đối với CSIRT quốc gia:
   . Các quy định và luật pháp sẽ ảnh hưởng đến hoạt động của nhóm
   . Các nguồn lực thiết yếu cần được xác định và bảo vệ
   . Những xu hướng và sự cố hiện tại đang được báo cáo hay cần phải báo cáo
   . Những năng lực đối phó sự cố và sự thành thạo về an ninh máy tính hiện có
b. Vạch ra tầm nhìn của CSIRT quốc gia
c. Vạch ra sứ mệnh của nhóm
d. Xác định đơn vị (hay các đơn vị) mà nó sẽ đáp ứng
e. Nhận diện các giao diện truyền thông giữa đơn vị và nhóm
f. Nhận diện các loại hình phê chuẩn quốc gia (chính phủ), bộ phận lãnh đạo và trách nhiệm của người đứng đầu

g. Nhận diện những kỹ năng và kiến thức của các nhân viên cần có để vận hành nhóm

h. Xác định vai trò và trách nhiệm của CSIRT quốc gia

i. Định rõ các quy trình quản lý sự cố của CSIRT cũng như các mối quan hệ với những quy trình tương tự trong bất kỳ một tổ chức đơn vị bên ngoài nào

j. Phát triển một bộ tiêu chuẩn hóa các tiêu chuẩn và thuật ngữ phù hợp cho việc phân loại và xác định những sự kiện và hoạt động xảy ra

k. Xác định xem CSIRT quốc gia sẽ tương tác như thế nào với đơn vị và các CSIRT trên thế giới khác hay các đối tác bên ngoài

l. Xác định những quá trình nào cần thiết cho việc tích hợp các kế hoạch đối phó sự cố, khôi phục thảm họa hiện tại, các kế hoạch hoạt động liên tục, quản lý khủng hoảng hay những kế hoạch quản lý khẩn cấp khác

m. Phát triển thời gian biểu cho dự án

n. Lập kế hoạch CSIRT quốc gia dựa trên các kết quả từ việc hoạch định khuôn khổ hoạt động, tầm nhìn và trách nhiệm

Giai đoạn 3 – Thực thi CSIRT

Trong giai đoạn 3, nhóm dự án sử dụng thông tin và kế hoạch có được từ giai đoạn 1 và giai đoạn 2 để thực thi CSIRT. Các quy trình thực thi như sau:

a. Thu thập các tài trợ từ những nguồn lực được xác định trong suốt giai đoạn hoạch định

b. Công bố rộng rãi rằng một CSIRT quốc gia sẽ được lập ra và nơi mà thông tin bổ sung có thể thu được (về quy trình phát triển, những yêu cầu báo cáo…)

c. Chính thức phối hợp và có các cơ chế tiếp xúc với các bên liên quan cũng như những đối tượng thích hợp khác

d. Thực thi cơ sở hạ tầng mạng lưới và những hệ thống thông tin đảm bảo nhằm vận hành CSIRT quốc gia (ví dụ như các máy chủ, ứng dụng, thiết bị viễn thông đảm bảo và những nguồn lực hỗ trợ cơ sở hạ tầng khác)

e. Xây dựng hoạt động và quy trình cho đội ngũ CSIRT, bao gồm tiêu chuẩn được phép trong giai đoạn hoạch định và hướng dẫn báo cáo

f. Xây dựng các thủ tục và chính sách nội bộ cho việc truy nhập và vận hành của thiết bị CSIRT và thiết bị cá nhân, cũng như các chính sách sử dụng chấp nhận được

g. Thực thi các quy trình tương tác của CSIRT quốc gia với các đơn vị thành viên của nó

h. Xác định và thuê (hay chuyển nhượng) nhân sự, có sự giáo dục và đào tạo thích hợp cho đội ngũ CSIRT, cũng như xác định những nỗ lực tiềm năng khác để giáo dục và đào tạo cho đơn vị thành viên

Giai đoạn 4 – Vận hành CSIRT

Ở giai đoạn vận hành, các dịch vụ cơ bản mà CSIRT quốc gia cung cấp được chỉ rõ và hiệu quả vận hành nhằm tận dụng năng lực quản lý sự cố được đánh giá. Dựa trên các kết quả, các chi tiết vận hành được xây dựng và cải tiến. Những hoạt động ở giai đoạn này bao gồm:

a. Chủ động thực hiện nhiều dịch vụ được cung cấp bởi CSIRT quốc gia

b. Phát triển và thực thi một cơ chế đánh giá hiệu quả các hoạt động của CSIRT quốc gia

c. Cải tiến CSIRT quốc gia theo những kết quả đánh giá

d. Mở rộng sứ mệnh, các dịch vụ và đội ngũ thích hợp và có thể duy trì lâu dài nhằm nâng cao dịch vụ cho đơn vị

e. Tiếp tục phát triển và nâng cao các thủ tục, chính sách CSIRT

Giai đoạn 5 – Cộng tác

Một CSIRT quốc gia có thể phát triển một mối quan hệ tin cậy với những bên liên quan chủ chốt thông qua các hoạt động hiệu quả (ở giai đoạn 4). Tuy nhiên, một SIRT quốc gia cũng có nhu cầu trao đổi các kinh nghiệm và thông tin quan trọng về quản lý sự cố thông qua trao đổi lâu dài với những cơ quan hợp tác, các CSIRT trong nước và CSIRT quốc tế. Các hoạt động ở giai đoạn này bao gồm:

a. Tham gia vào các hoạt động chia sẻ thông tin và dữ liệu đồng thời hỗ trợ sự phát triển những tiêu chuẩn đối với việc chia sẻ thông tin và dữ liệu giữa các đối tác, các CSIRT khác, các đơn vị cấu thành và các chuyên gia an ninh máy tính khác

b. Tham gia vào các chức năng ‘theo dõi và cảnh báo’ toàn cầu nhằm hỗ trợ cho cộng đồng các CSIRT

c. Cải thiện chất lượng các hoạt động của CSIRT bằng cách tổ chức những buổi hội nghị, hội thảo và đào tạo thảo luận về các xu hướng tấn công và các chiến lược đối phó

d. Cộng tác với những đơn vị khác trong cộng đồng nhằm xây dựng các hướng dẫn và tài liệu thực tiễn tốt nhất

e. Xem xét lại và sửa đổi các tiến trình quản lý sự cố như một phần tiếp theo của quá trình phát triển

Các dịch vụ CSIRT[54]

Những dịch vụ mà CSIRT cung cấp có thể phân chia thành các dịch vụ tác động trở lại, các dịch vụ tiên phong và các dịch vụ quản lý dịch vụ.

Các dịch vụ tác động trở lại (Reactive services) là những dịch vụ cốt lõi của một CSIRT. Chúng bao gồm:

1. Báo động và cảnh báo – Dịch vụ này bao gồm việc cung cấp thông tin và các phương pháp để đối phó với những vấn đề như một nguy cơ tấn công an ninh, một báo động xâm nhập, một virus máy tính hay đánh lừa.
2. Quản lý sự cố - Dịch vụ này liên quan đến việc tiếp nhận, chọn lọc và đáp ứng lại những yêu cầu cũng như báo cáo, phân tích và dành ưu tiên đối với các sự kiện và sự cố. Những hoạt động đối phó bao gồm:
   - Phân tích sự cố - Một bước kiểm tra đối với tất cả thông tin sẵn có và dấu hiệu hỗ trợ hay có liên quan đến một sự kiện hoặc sự cố. Mục đích của việc phân tích là nhằm xác định phạm vi của sự cố, quy mô của thiệt hại gây ra bởi sự cố, bản chất của sự cố và những chiến lược đối phó hay biện pháp khắc phục sẵn có.
   - Thu thập các bằng chứng pháp luật – Thu thập, bảo quản, lập tài liệu và phân tích về chứng cứ từ một hệ thống máy tính bị hại nhằm xác định các thay đổi đối với hệ thống và nhằm hỗ trợ trong quá trình xây dựng lại những sự kiện dẫn đến sự cố bị hại này.
   - Theo dõi hay lần theo dấu vết – Liên quan tới việc theo dõi hay lần tìm xem kẻ xâm nhập đi vào hệ thống và các mạng liên quan như thế nào. Hoạt động này bao gồm việc lần theo lai lịch của một kẻ xâm nhập hay phân tích hệ thống mà kẻ xâm nhập đó đã truy cập.

[54] Được trích trong Carnegie Mellon University, CSIRT Services (2002), http://www.cert.org/archive/pdf/CSIRT-services-list.pdf.

3. Đối phó sự cố tại địa điểm – CSIRT đưa ra định hướng, hỗ trợ tại đơn vị nhằm giúp đỡ các đơn vị khôi phục lại sự cố.
4. Hỗ trợ đối phó sự cố - CSIRT hỗ trợ và hướng dẫn (các) đối tượng bị hại của cuộc tấn công trong việc khôi phục từ một sự cố thông qua điện thoại, e-mail, fax, hay tài liệu.
5. Điều phối việc đối phó sự cố - Các nỗ lực đối phó giữa các bên liên quan trong một sự cố thì được điều phối. Nó thường bao gồm đối tượng bị hại của cuộc tấn công, các đơn vị liên quan khác trong vụ tấn công và bất kỳ đơn vị nào yêu cầu hỗ trợ trong việc phân tích về cuộc tấn công. Nó cũng có thể bao gồm các bên cung cấp sự hỗ trợ IT cho đối tượng bị hại như các ISP và những CSIRT khác.
6. Quản lý khả năng bị tấn công – Dịch vụ này liên quan đến việc tiếp nhận thông tin và báo cáo về cá khả năng bị tấn công phần mềm và phần cứng, phân tích những tác động của khả năng bị tấn công, đồng thời phát triển các chiến lược đối phó đối với việc dò tìm và sửa chữa các khả năng bị tấn công.
   . Phân tích khả năng bị tấn công – Chỉ việc kiểm tra và phân tích mặt vật lý về các khả năng bị tấn công phần cứng và phần mềm. Công tác phân tích có thể bao gồm việc xem xét mã nguồn, sử dụng chương trình sửa lỗi nhằm xác định địa điểm xảy ra khả năng bị tấn công, hoặc cố gắng tái tạo lại trên một hệ thống kiểm thử.
   . Đối phó với khả năng bị tấn công – Liên quan đên việc xác định biện pháp đối phó thích hợp nhằm giảm nhẹ hoặc sửa chữa khả năng bị tấn công. Dịch vụ này bao gồm việc thực hiện biện pháp đối phó bằng cách cài đặt các bản vá, sửa lỗi hay khắc phục. Nó cũng bao gồm việc thông báo về các chiến lược giảm nhẹ, những cố vấn hay các cảnh báo.
   . Cộng tác đối phó với khả năng bị tấn công – CSIRT thông báo tới rất nhiều bộ phận của tổ chức hay đơn vị thành viên về khả năng bị tấn công và chia sẻ thông tin làm thế nào để sửa lỗi hay giảm thiểu nó. CSIRT cũng phân loại những chiến lược đối phó hiệu quả đối với khả năng bị tấn công. Các hoạt động bao gồm việc phân tích khả năng bị tấn công hay báo cáo khả năng bị tấn công đồng thời tổng hợp những phân tích kỹ thuật được thực hiện bởi các bên khác nhau. Dịch vụ này cũng có thể bao gồm việc duy trì tri thức hay tài liệu lưu

trữ công cộng hoặc cá nhân dựa trên thông tin và những chiến lược đối phó phù hợp khả năng bị tấn công.

7. Quản lý sự biến đổi – Bao gồm việc phân tích, đối phó, điều phối và quản lý những biến đổi liên quan tới virus máy tính, các chương trình Trojan, sâu, bộ công cụ và mã khai thác.
   - Phân tích sự biến đổi – CSIRT thực hiện việc phân tích và kiểm tra kỹ thuật về bất kỳ sự thay đổi nào tìm thấy trong một hệ thống.
   - Đối phó sự biến đổi – Liên quan đến việc xác định các hành động thích hợp nhằm tìm ra và tháo gỡ các biến đổi trong một hệ thống.
   - Cộng tác đối phó sự biến đổi – Liên quan đến việc chia sẻ và tổng hợp các kết quả phân tích cũng như các chiến lược đối phó đi liền với một sự biến đổi với các nhà nghiên cứu, các CSIRT, các bên bán hàng và các chuyên gia an ninh khác.

Các dịch vụ tiên phong là nhằm cải thiện cơ sở hạ tầng và các quy trình an ninh của đơn vị thành viên trước khi bất kỳ sự cố hay sự kiện nào xảy ra được phát hiện. Chúng bao gồm:

1. Việc thông báo – Bao gồm báo động xâm nhập, cảnh báo nguy cơ bị tấn công, các cố vấn an ninh và những vấn đề tương tự. Cũng như các thông báo được truyền tới những đơn vị thành viên về những phát triển mới với tác động trung và dài hạn, ví dụ các khả năng bị tấn công hay các công cụ xâm nhập mới được phát hiện. Các thông cáo cho phép những đơn vị thành viên bảo vệ mạng lưới và hệ thống của mình chống lại các vấn đề vừa phát hiện trước khi chúng có thể bị khai thác.
2. Theo dõi về công nghệ - Liên quan đến việc theo dõi và giám sát sự phát triển công nghệ mới, các hoạt động thâm nhập và những xu hướng liên quan nhằm giúp xác định những mối đe dọa tương lai. Kết quả từ dịch vụ này có thể là một số loại hướng dẫn hay khuyến nghị tập trung nhiều hơn vào các vấn đề an ninh trung và dài hạn.
3. Đánh giá và kiểm tra an ninh – Dịch vụ này cung cấp phân tích và xem xét lại một cách chi tiết về hạ tầng an ninh của một tổ chức, dựa trên những yêu cầu được xác định bởi tổ chức hoặc các tiêu chuẩn ngành khác được áp dụng.

4. Cấu hình và bảo trì các công cụ, ứng dụng, hạ tầng và dịch vụ an ninh – Dịch vụ này đưa ra chỉ dẫn thích hợp làm thế nào để cấu hình và bảo trì một cách an toàn cho các công cụ, ứng dụng và hạ tầng máy tính nói chung.
5. Phát triển các công cụ an ninh – Dịch vụ này bao gồm việc phát triển các công cụ, phần mềm, chương trình đi kèm cũng như các bản vá được xây dựng và phân phối cho mục đích an ninh.
6. Dịch vụ dò tìm xâm nhập – Các CSIRT thực hiện dịch vụ này xem xét lại bản ghi IDS (IDS log), phân tích chúng và đề xuất một biện pháp đối phó với các sự kiện phù hợp với điểm ngưỡng được xác định của chúng.
7. Phổ biến thông tin liên quan đến an ninh – Dịch vụ này cung cấp cho các đơn vị thành viên một tập hợp toàn diện và dễ dàng tìm kiếm về thông tin hữu ích giúp cho việc nâng cao an ninh.

Các dịch vụ quản lý chất lượng an ninh được thiết kế nhằm cung cấp kiến thức thu được từ công tác đối phó với sự cố, nguy cơ bị tấn công và các cuộc tấn công một cách đồng bộ. Dịch vụ này bao gồm:

1. Phân tích rủi ro – Liên quan tới việc cải thiện năng lực của CSIRT nhằm đánh giá các mối đe dọa thực, đưa ra những đánh giá về số lược và chất lượng mang tính thực tế về những rủi ro đối với các tài sản thông tin, đồng thời đánh giá về các chiến lược đối phó và bảo vệ.
2. Lên kế hoạch khôi phục thảm họa và hoạt động một cách liên tục – Khôi phục và đảm bảo hoạt động liên tục từ các thảm họa gây ra bởi các cuộc tấn công an ninh máy tính được bảo đảm thông qua kế hoạch đầy đủ.
3. Cố vấn an ninh – Các CSIRT cũng có thể đưa ra những chỉ dẫn hay lời lời khuyên thực tế đối với các hoạt động kinh doanh.
4. Tạo dựng nhận thức – Các CSIRT có thể nâng cao nhận thức về an ninh bằng cách xác định và cung cấp thông tin và chỉ dẫn về những chính sách và thực tiễn an ninh mà các đơn vị thành viên yêu cầu.
5. Giáo dục/Đào tạo – Dịch vụ này liên quan đến việc cung cấp các khóa giáo dục và đào tạo về những chủ đề như các chỉ dẫn báo cáo sự cố, các phương pháp đối phó thích hợp, các công cụ đối phó sự cố,

phương pháp ngăn ngừa sự cố và thông tin cần thiết khác để bảo vệ, dò tìm, báo cáo và đối phó các sự cố an ninh máy tính. Những phương thức đào tạo bao gồm các buổi hội nghị chuyên đề, hội thảo, khóa học và những buổi hướng dẫn.

6. Đánh giá hay chứng nhận sản phẩm – CSIRT có thể chỉ đạo việc đánh giá sản phẩm đối với các công cụ, ứng dụng hay những dịch vụ khác nhằm đảm bảo sự an toàn của các sản phẩm cũng như tính phù hợp của chúng để CSIRT có thể chấp nhận được hay thực tiễn an ninh của tổ chức.

Bảng 12 thể hiện mức độ của mỗi dịch vụ CSIRT – ví dụ đâu là dịch vụ cốt lõi (core), dịch vụ cộng thêm (additional) hay dịch vụ đặc sắc (unusual) – trong mỗi mô hình CSIRT.

Bảng 12. Các dịch vụ CSIRT

Loại dịch vụ	**Các dịch vụ**		**Nhóm an ninh**	**Phân tán**	**Tập trung**	**Kết hợp**	**Điều phối**
Tác động trở lại	Báo động và cảnh báo		Additional	Core	Core	Core	Core
	Quản lý sự cố	Phân tích sự cố	Core	Core	Core	Core	Core
		Đối phó sự cố tại địa điểm	Core	Additional	Additional	Additional	Unusual
		Hỗ trợ đối phó sự cố	Unusual	Core	Core	Core	Core
		Điều phối việc đối phó sự cố	Core	Core	Core	Core	Core
	Quản lý sự biến đổi	Phân tích khả năng bị tấn công	Additional	Additional	Additional	Additional	Additional
		Đối phó với khả năng bị tấn công	Core	Additional	Unusual	Additional	Additional
		Cộng	Additional	Core	Core	Core	Core

		tác đối phó với khả năng bị tấn công					
		Phân tích sự biến đổi	Additional	Additional	Additional	Additional	Additional
		Đối phó sự biến đổi	Core	Additional	Additional	Additional	Additional
		Cộng tác đối phó sự biến đổi	Additional	Additional	Core	Core	Core
Tiên phong	Thông báo		Unusual	Core	Core	Core	Core
	Theo dõi về công nghệ		Unusual	Additional	Core	Core	Core
	Đánh giá và kiểm tra an ninh		Unusual	Additional	Additional	Additional	Additional
	Cấu hình và bảo trì các công cụ, ứng dụng, hạ tầng và dịch vụ an ninh		Core	Additional	Additional	Additional	Unusual
	Phát triển các công cụ an ninh		Additional	Additional	Additional	Additional	Additional
	Dịch vụ dò tìm xâm nhập		Core	Additional	Additional	Additional	Unusual
	Phổ biến thông tin liên quan đến an ninh		Unusual	Additional	Core	Core	Core
Quản lý chất lượng an ninh	Phân tích rủi ro		Unusual	Additional	Additional	Additional	Additional
	Lên kế hoạch khôi phục thảm họa và hoạt động một cách liên tục		Unusual	Additional	Additional	Additional	Additional
	Cố vấn an ninh		Unusual	Additional	Additional	Additional	Additional
	Tạo dựng nhận thức		Unusual	Additional	Additional	Additional	Core
	Giáo dục/Đào tạo		Unusual	Additional	Additional	Additional	Core
	Đánh giá hay chứng nhận sản phẩm		Unusual	Additional	Additional	Additional	Additional

Nguồn: Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle and Mark Zajicek, Organizational Models for Computer Security Incident Response Teams (CSIRTs) (Pittsburgh: Carnegie Mellon University, 2003), http://www.cert.org/archive/pdf/03hb001.pdf.

6.2. Các cơ quan CSIRT quốc tế

Hiện tại, có một số CSIRT quốc tế chuyên dụng được thiết lập để đối phó với những sự cố an ninh máy tính trên toàn thế giới. Trong khi các CSIRT quốc gia có thể đối mặt với những cuộc tấn công và thực hiện các chức năng khác của mình, một cuộc tấn công quốc tế đòi hỏi sự tham gia của một CSIRT quốc tế.

Diễn đàn của các Nhóm an ninh và đối phó sự cố (Forum of Incident Response Security Teams – FIRST)[55]

FIRST bao gồm các CERT, các cơ quan chính phủ và công ty an ninh của 41 quốc gia. Thành viên của nó có 191 tổ chức, gồm có CERT/CC và US-CERT. FIRST là một đơn vị điều phối và chia sẻ thông tin giữa các nhóm đối phó sự cố. Mục đích của nó là nhằm chủ động trong các hoạt động bảo vệ và đối phó sự cố, đồng thời thúc đẩy sự cộng tác giữa các thành viên thông qua việc cung cấp cho họ công nghệ, kiến thức và những công cụ cho việc đối phó sự cố. Những hoạt động của FIRST bao gồm:

- Xây dựng và chia sẻ các bài học thực tiễn tốt nhất, thủ tục, công cụ, những phương pháp và thông tin kỹ thuật cho việc bảo vệ và đối phó sự cố;
- Thúc đẩy việc phát triển các chính sách, dịch vụ và sản phẩm an ninh chất lượng tốt;
- Hỗ trợ và phát triển những chỉ dẫn an ninh máy tính phù hợp;
- Giúp đỡ các chính phủ, doanh nghiệp và đơn vị giáo dục để xây dựng một nhóm đối phó sự cố và mở rộng nó; và
- Tạo điều kiện thuận lợi cho việc chia sẻ công nghệ, kinh nghiệm và kiến thức giữa các thành viên cho một môi trường điện tử an toàn hơn.

Cơ quan CERT Châu Á Thái Bình Dương (Asia Pacific CERT)[56]

Nhóm phản ứng khẩn cấp máy tính Châu Á Thái Bình Dương (Asia-Pacific Computer Emergency Response Team - APCERT) được thành lập tháng 2/2003 nhằm đáp ứng như một mạng lưới những chuyên gia an ninh, tăng cường khả năng đối phó sự cố và nâng cao nhận thức về an ninh trong khu vực Châu Á Thái Bình Dương. Hội nghị đầu tiên của Asia Pacific CERT được tổ chức tại

[55] FIRST, "About FIRST," FIRST.org, Inc., http://www.first.org/about/.
[56] APCERT, "Background," http://www.apcert.org/about/background/index.html.

Nhật Bản năm 2002. Cuối năm, APCERT đã tài trợ cho một hội nghị tại Taipei, thu hút sự tham gia của 14 cơ quan Asia Pacific CERT. Tính đến tháng 8/2007, APCERT có 14 thành viên chính thức và 6 thành viên cộng tác.

Các thành viên APCERT nhất trí rằng những sự cố an ninh máy tính ngày nay quá nhiều, phức tạp và khó có thể kiểm soát đối với bất kỳ một tổ chức hay một quốc gia nào, và một biện pháp đối phó hiệu quả hơn có thể được triển khai thông qua sự cộng tác với những thành viên khác của APCERT. Như trong FIRST, khái niệm quan trọng nhất trong APCERT là mối quan hệ tin cậy giữa các thành viên trong việc trao đổi thông tin và cộng tác với mỗi thành viên khác. Do đó, các hoạt động của APCERT được xây dựng nhằm:

- Nâng cao sự hợp tác quốc tế và khu vực Châu Á – Thái Bình Dương;
- Tham gia phát triển những biện pháp phù hợp với các sự cố an ninh mạng lưới khu vực hoặc trên phạm vi rộng;
- Tăng cường chia sẻ thông tin an ninh và trao đổi công nghệ, bao gồm thông tin về virus máy tính, các đoạn mã khai thác và những vấn đề tương tự;
- Tăng cường hợp tác nghiên cứu về những vấn đề chung;
- Giúp đỡ các cơ quan CIRT khác trong khu vực trong việc đối phó hiệu quả với những sự cố an ninh máy tính; và
- Đưa ra các giải pháp và chỉ dẫn đối với những vấn đề luật pháp có liên quan tới đối phó sự cố và an ninh thông tin khu vực.

Cơ quan CERT của chính phủ Châu Âu (European Government CERT)[57]

European Government CERT (EGC) là một ủy ban không chính thức được hỗ trợ cùng với những cơ quan CERT của các quốc gia Châu Âu. Các thành viên của nó bao gồm Hà Lan, Pháp, Đức, Hungary, Netherlands, Na Uy, Thụy Điển, Thụy Sĩ và Anh. Vai trò và trách nhiệm của cơ quan này là nhằm:

- Tham gia phát triển những biện pháp phù hợp với các sự cố an ninh mạng lưới khu vực hoặc trên phạm vi rộng;
- Đẩy mạnh chia sẻ thông tin và trao đổi công nghệ về sự cố an ninh cũng như các mối đe dọa mã độc và khả năng bị tấn công;

[57] EGC, http://www.egc-group.org.

- Xác định phạm vi của kiến thức và ý kiến chuyên môn có thể được chia sẻ trong nhóm;
- Xác định phạm vi hợp tác nghiên cứu và phát triển những mục tiêu quan tâm của các thành viên; và
- Đẩy mạnh thông tin của các CSIRT chính phủ trong các quốc gia Châu Âu.

Cơ quan An ninh Thông tin và Mạng lưới Châu Âu (European Network and Information Security Agency - ENISA)[58]

Mục đích của ENISA là nhằm nâng cao an ninh mạng lưới và an ninh thông tin trong Liên minh Châu Âu thông qua việc tạo lập văn hóa NIS. Cơ quan này được thiết lập tháng 1/2004 bởi Hội đồng Bộ trưởng và Quốc hội Châu Âu nhằm đối phó với tội phạm 'hi-tech'. Nó thực hiện những vai trò sau đây:

- Cung cấp sự hỗ trợ nhằm đảm bảo NIS giữa các thành viên của ENISA và EU;
- Đẩy mạnh trao đổi bền vững về thông tin giữa các bên liên quan; và
- Tăng cường cộng tác về những chức năng liên quan đến NIS.

ENISA được mong đợi sẽ đóng góp vào các nỗ lực quốc tế nhằm giảm bớt virus và hacking, đồng thời thiết lập công tác giám sát trực tuyến đối với các mối đe dọa.

6.3. Các cơ quan CSIRT quốc gia

Một số nước có một CSIRT quốc gia. Bảng 13 liệt kê những quốc gia và CSIRT tương ứng của họ cũng như địa chỉ website cho mỗi đơn vị.

Bảng 13. Danh sách các cơ quan CSIRT quốc gia

Quốc gia	Tên cơ quan	Trang chủ
Argentina	Computer Emergency Response Team of the Argentine Public Administration	http://www.arcert.gov.ar
Australia	Australia Computer Emergency Response Team	http://www.aucert.org.au
Brazil	Computer Emergency Response Team Brazil	http://www.cert.br
Brunei Darussalam	Brunei Computer Emergency Response Team	http://www.brucert.org.bu

[58] ENISA, "About ENISA," http://www.enisa.europa.eu/pages/About_ENISA.htm.

Quốc gia	Tên cơ quan	Trang chủ
Canada	Public Safety Emergency Preparedness Canada	http://www.psepc-sppcc.gc.ca/prg/em/ccirc/index-en.asp
Chile	Chilean Computer Emergency Response Team	http://www.clcert.cl
China	National Computer Network Emergency Response Technical Ream - Coordination Center of China	http://www.cert.org.cn
Denmark	Danish Computer Emergency Response Team	http://www.cert.dk
El Salvador	Response Team for Computer Security Incidents	
Finland	Finnish Communication Regulatory Authority	http://www.cert.fi
France	CERT-Administration	http://www.certa.ssi.gouv.fr
Germany	CERT-Bund	http://www.bsi.bund.de/certbund
Hong Kong	Hong Kong Computer Response Coordination Centre	http://www.hkcert.org
Hungary	CERT-Hungary	http://www.cert-hungary.hu
India	CERT-In	http://www.cert-in.org.in
Indonesia	Indonesia Computer Emergency Response Team	http://www.cert.or.id
Japan	JP CERT Coordination Center	http://www.jpcert.or.jp
Lithiania	LITNET CERT	http://cert.litnet.lt
Malaysia	Malaysian Computer Emergency Response Team	http://www.mycert.org.my
Mexico	Universidad Nacional Autonoma de Mexico	http://www.cert.org.mx
Netherlands	GOVCERT.NL	http://www.govcert.nl
New Zealand	Centre for Critical Infrastructure Protection	http://www.ccip.govt.nz
Norway	Norwegian National Security Authority	http://www.cert.no
Philippines	Philippines Computer Emergency Response Team	http://www.phcert.org
Poland	Computer Emergency Response Team Polska	http://www.cert.pl
Qatar	Qatar Computer Emergency Response Team	http://www.qcert.org
Saudi Arabia	Computer Emergency Response Team - Saudi Arabia	http://www.cert.gov.sa
Singapore	Singapore Computer Emergency Response Team	http://www.singcert.org.sg
Slovenia	Slovenia Computer Emergency Response Team	http://www.arnes.si/english/si-cert
Republic of Korea	CERT Coordination Center Korea	http://www.krcert.or.kr
Spain	IRIS-CERT	http://www.rediris.es/cert
Sweden	Swedish IT Incident Centre	http://www.sitic.se
Thailand	Thai Computer Emergency Response Team	http://www.thaicert.nectec.or.th
Tunisia	Computer Emergency Response	http://www.ansi.tn/en/about_cert-

Quốc gia	Tên cơ quan	Trang chủ
	Team - Tunisian Coordination Center	tcc.htm
Turkey	TP-CERT	http://www.uekae.tubitak.gov.tr
United Kingdom	GovCertUK	http://www.govcertuk.gov.uk
United States	United States -Computer Emergency Response Team	http://www.us-cert.gov
Viet Nam	Viet Nam Computer Emergency Response Team	http://www.vncert.gov.vn

Nguồn: CERT, "National Computer Security Incident Response Teams," Carnegie Mellon University, http://www.cert.org/csirts/national/contact.html.

Bài tập

Có cơ quan CSIRT quốc gia nào ở đất nước bạn hay không?

1. Nếu có, hãy mô tả về mô hình mà nó áp dụng theo và cách thức hoạt động của nó. Đánh giá hiệu quả thực thi các chức năng của nó.
2. Nếu không, xác định mô hình CSIRT có thể sẽ phù hợp với đất nước bạn và mô tả cái gì là yêu cầu đối với việc thiết lập một CSIRT quốc gia tại đất nước bạn.

Tự kiểm tra

1. Những chức năng chính của các CSIRT là gì?
2. Đâu là sự khác nhau giữa những CSIRT quốc tế và CSIRT quốc gia?
3. Những yêu cầu đối với việc thiết lập một CSIRT là gì?

7. VÒNG ĐỜI CỦA CHÍNH SÁCH AN NINH THÔNG TIN

Phần này nhằm mục đích:

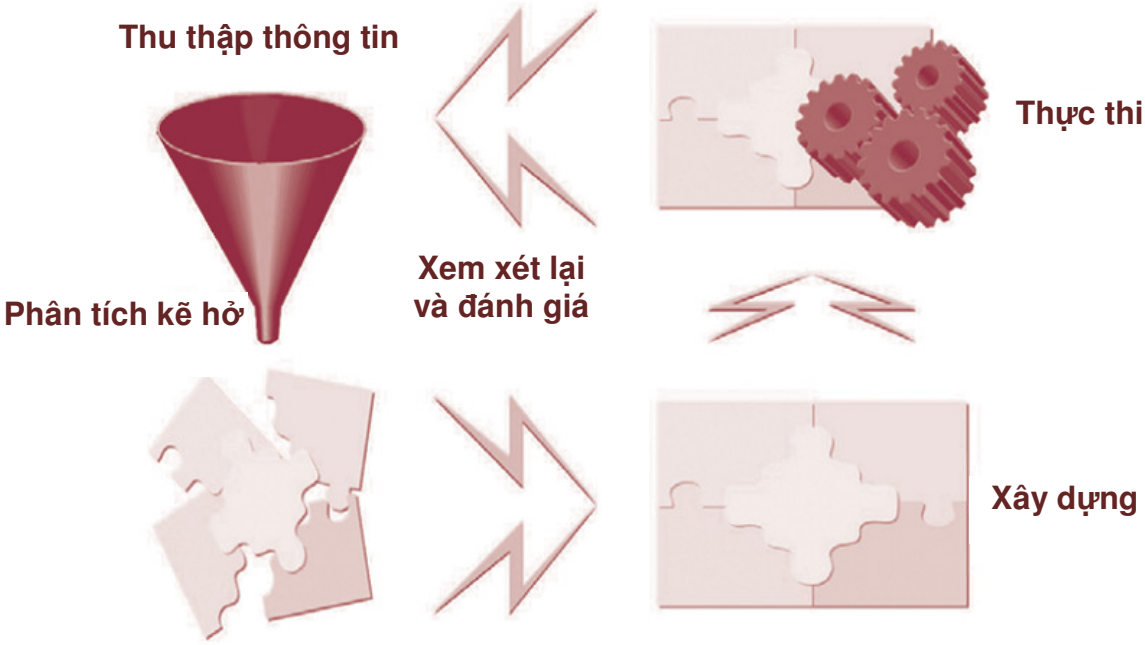
- **Đưa ra cái nhìn tổng quan về quy trình tạo lập chính sách an ninh thông tin; và**
- **Thảo luận những vấn đề mà các nhà lập chính sách phải xem xét trong quá trình xây dựng chính sách an ninh thông tin.**

Những nhà lập chính sách cần đưa vào tính toán một số cân nhắc, trong đó có những nhân tố căn bản đối với một chính sách, những nguồn lực sẵn có, định hướng chính sách, các yêu cầu về luật pháp và ngân sách, và kết quả đầu ra về chính sách mong đợi. Trong phần này, những cân nhắc này được thảo luận trong ngữ cảnh của các giai đoạn khác nhau của việc xây dựng chính sách an ninh thông tin.

Cần chú ý rằng các quốc gia khác nhau sẽ có đôi chút khác nhau về ngữ cảnh cũng như sự cân nhắc về chính sách. Quá trình xây dựng chính sách được mô tả trong phần này là chung nhất và được dựa trên giả định rằng hiện chưa có chính sách an ninh thông tin quốc gia nào.

Cũng như những chính sách khác, vòng đời của chính sách an ninh thông tin có thể được chia thành 4 pha: (1) thu thập thông tin và phân tích kẽ hở; (2) xây dựng chính sách; (3) thực thi chính sách; (4) kiểm soát và tiếp nhận phản hồi (Hình 19). Ngoài ra, một chính sách an ninh thông tin quốc gia cần có chiến lược an ninh thông tin, các mối quan hệ luật pháp, tổ chức an ninh thông tin, công nghệ an ninh thông tin, và những mối quan hệ bên trong của chúng.

Hình 19. Vòng đời của chính sách an ninh thông tin



7.1. Thu thập thông tin và phân tích kẽ hở

Giai đoạn đầu tiên trong quá trình xây dựng một chính sách an ninh thông tin là thu thập thông tin và phân tích kẽ hở.

Trong thu thập thông tin, một điều hữu ích là xem xét các ví dụ về an ninh thông tin và những chính sách liên quan của các quốc gia khác, cũng như những chính sách liên quan của bản thân quốc gia đó.

Trong phân tích kẽ hở, một điều quan trọng là nắm bắt được yếu tố hạ tầng hiện có liên quan đến an ninh thông tin, như các hệ thống và pháp luật hiện tại, những lĩnh vực và kẽ hở cần được hoàn thiện. Đây là một bước quan trọng vì nó xác định định hướng và ưu tiên trong chính sách an ninh thông tin sẽ được thiết lập.

Thu thập thông tin

Thu thập các trường hợp từ nước ngoài: Trong việc xác định các trường hợp liên quan từ những quốc gia khác, các nhà hoạch định chính sách cần xem xét các yếu tố tương tự trong:

- Mức độ an ninh thông tin quốc gia
- Định hướng xây dựng chính sách
- Hạ tầng hệ thống và mạng lưới

Xem xét những yếu tố tương tự này, cần thu thập các dữ liệu sau:

- Thông tin về việc xây dựng và vận hành của các tổ chức liên quan đến an ninh thông tin (xem chương 3 và chương 6 của học phần này)
- Thông tin về các chính sách, luật pháp, và các quy định về an ninh (xem chương 3)
- Phương pháp an ninh thông tin được sử dụng trên phạm vi quốc tế và những ví dụ từ các quốc gia khác (xem chương 4)
- Các xu hướng đe dọa và những biện pháp đối phó hay kiểm soát theo các loại hình tấn công (xem các chương 2 và 6)
- Các biện pháp đối phó cho việc bảo vệ bí mật riêng tư (xem chương 5)

Thu thập các dữ liệu trong nước: Mặc dù hầu hết những nhà hoạch định chính sách không phải là chuyên gia trong lĩnh vực an ninh thông tin, họ có thể thực hiện những hoạt động có liên quan hay đi liền với an ninh thông tin. Một cách cụ thể, họ tham gia xây dựng luật pháp, quy định và chính sách trong các lĩnh vực liên quan đến an ninh thông tin. Tuy nhiên, do luật pháp, quy định và chính sách có khuynh hướng tập trung vào các lĩnh vực nhất định, sự tương quan giữa chúng có thể không hiện ra ngay tức thì đối với những nhà hoạch định chính sách. Vì vậy, cần tiến hành thu thập, phân tích và đánh giá tất cả những luật pháp, quy định và chính sách có liên quan hay đi liền với an ninh thông tin.

Phân tích kẽ hở

Tác phẩm *The Art of War* của Sun Tzu nói rằng "Cần nắm bắt kẻ thù của bạn". Điều này có nghĩa là bạn cần phải biết được những giới hạn của mình cũng như đó là kẻ thù của bạn. Trong trường hợp xây dựng chính sách an ninh thông tin, điều này có nghĩa là cần biết được cái gì cần thiết được bảo vệ thông qua một chính sách an ninh thông tin cũng như khả năng bị tấn công và những mối đe dọa đối với an ninh thông tin.

Phân tích kẽ hở có thể được chia thành hai pha:

1. Nắm bắt được các năng lực và khả năng của quốc gia – ví dụ như các nguồn lực con người và tổ chức, cũng như cơ sở hạ tầng thông tin và truyền thông – trong lĩnh vực an ninh thông tin; và
2. Xác định các mối đe dọa từ bên ngoài đối với an ninh thông tin.

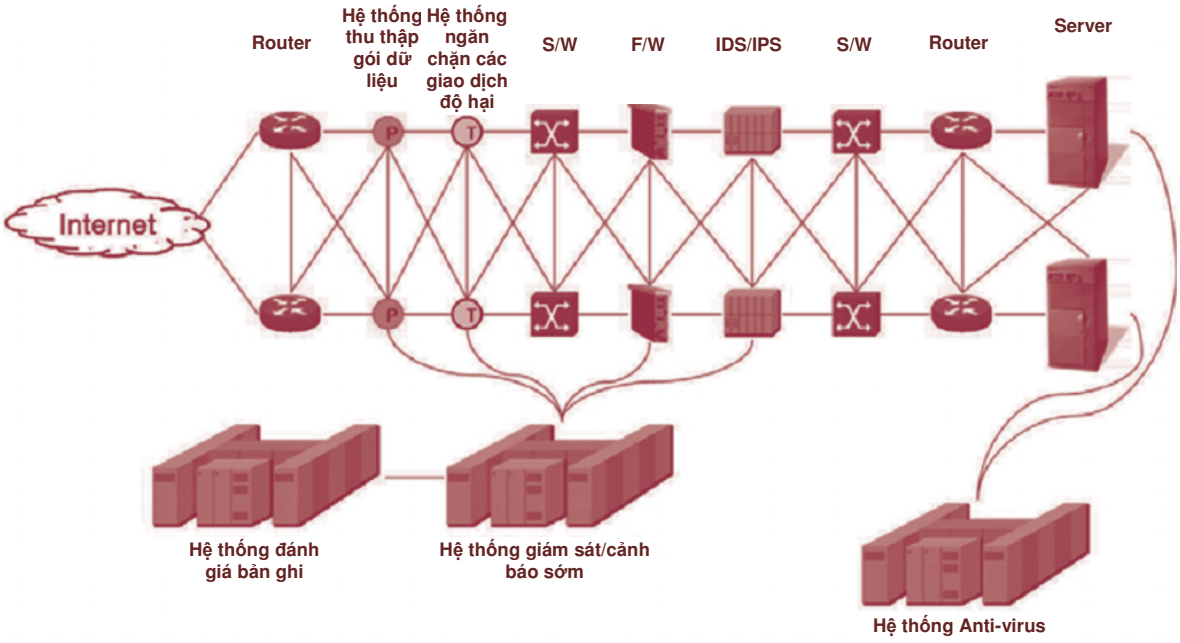
Những nhà hoạch định chính sách cần **biết rõ các nguồn lực con người và tổ chức an ninh thông tin** – ví dụ các cơ quan tư nhân và công cộng trong

các lĩnh vực liên quan đến an ninh thông tin. Họ cần biết những tổ chức liên quan trong hoạt động an ninh thông tin và nắm bắt được phạm vi hoạt động, vai trò, trách nhiệm của các tổ chức này. Điều này là quan trọng nhằm tránh trùng lặp các cấu trúc đã có về an ninh thông tin.

Cũng tại điểm này, những chuyên gia về an ninh thông tin cần được nhận diện và đặt mối quan hệ. Bởi các chuyên gia thường có một nền về tảng luật pháp, chính sách, công nghệ, giáo dục và những lĩnh vực có liên quan.

Cơ sở hạ tầng thông tin – truyền thông đề cập đến cấu trúc IT như việc thu thập, xử lý, lưu trữ, tìm kiếm, truyền tải và tiếp nhận thông tin và các hệ thống quản lý điều khiển điện tử. Nói ngắn gọn, đây là mạng lưới và hệ thống thông tin. **Nắm bắt hiện trạng của cơ sở hạ tầng thông tin – truyền thông** là đặc biệt quan trong từ quan điểm kinh tế. Bởi những khoản đầu tư lớn cần được kết nối toàn bộ đất nước, làm cho các phương tiện thông tin – truyền thông hiện có trở nên tiện lợi. Hình 20 đưa ra một ví dụ về cơ sở hạ tầng thông tin – truyền thông cho vấn đề an ninh thông tin. Nó không bao hàm tất cả những chi tiết có thể được yêu cầu và ví dụ được đưa ra ở đây chỉ nhằm mục đích minh họa. Lưu ý mối quan hệ giữa rất nhiều thành phần trong mạng lưới.

Hình 20. Ví dụ về cấu trúc hệ thống và mạng lưới



Những nhà hoạch định chính sách cần hiểu được các hệ thống và mạng lưới chung về an ninh thông tin được bố trí như thế nào.

Bước thứ hai trong phân tích kẽ hở đó là **xác định các mối đe dọa bên ngoài đối với an ninh thông tin**. Như đã đề cập trong chương 2, các mối đe dọa

đối với an ninh thông tin không chỉ tăng lên mà còn phức tạp hơn. Các nhà lập chính sách cần hiểu những mối đe dọa này để có thể quyết định biện pháp đối phó nào là cần thiết. Nói một cách cụ thể, các nhà lập chính sách cần phải hiểu:

- Tốc độ thâm nhập của các mối đe dọa đối với an ninh thông tin
- Các loại hình tấn công hiện tại và phổ biến nhất
- Các loại hình đe dọa và mức độ dự kiến về sức mạnh của chúng trong tương lai

Sau khi phân tích các nguồn lực con người, tổ chức quốc gia và cơ sở hạ tầng thông tin – truyền thông, cũng như nắm bắt các nhân tố đe dọa trong lĩnh vực an ninh thông tin, một điều quan trọng đó là tìm ra được nguyên nhân từ các yếu tố có thể bị tấn công. Điều này sẽ xác định được phạm vi mà theo đó quốc gia có thể chống lại các thành phần đe dọa bên ngoài. Việc xác định có thể được thực hiện thông qua kiểm tra những vấn đề sau đây:

- Hiện trạng của CERT và khả năng đối phó của nó
- Hiện trạng của các chuyên gia về an ninh thông tin
- Mức độ xây dựng và sức mạnh của hệ thống an ninh thông tin
- Quy phạm pháp luật bảo vệ chống lại sự xâm phạm tài sản thông tin
- Môi trường vật lý cho việc bảo vệ các tài sản thông tin

Mục tiêu của việc phân tích kẽ hở là nhằm có thể xác định các biện pháp đối phó thực tiễn cần được thực hiện. Cần nhấn mạnh rằng đây là bước cơ bản nhất trong việc hoạch định chính sách an ninh thông tin.

7.2. Xây dựng chính sách an ninh thông tin

Việc xây dựng một chính sách an ninh thông tin liên quan tới: (1) vạch ra định hướng chính sách; (2) thiết lập tổ chức an ninh thông tin và xác định trách nhiệm cũng như vai trò của nó; (3) kết nối khuôn khổ chính sách an ninh thông tin; (4) xây dựng và/hoặc sửa lại luật pháp giúp tạo cho chúng sự thích hợp với chính sách; và (5) phân bổ một nguồn ngân sách cho việc thực hiện chính sách thông tin.

1. Thiết lập định hướng chính sách và đẩy mạnh tiến về phía trước

Trong hầu hết các trường hợp, việc theo đuổi chính sách an ninh thông tin cần được đi đầu bởi chính phủ hơn là để cho khu vực tư nhân. Đặc biệt, chính phủ cần thiết lập chính sách, đóng vai trò trong việc dẫn đầu đưa cơ sở hạ tầng

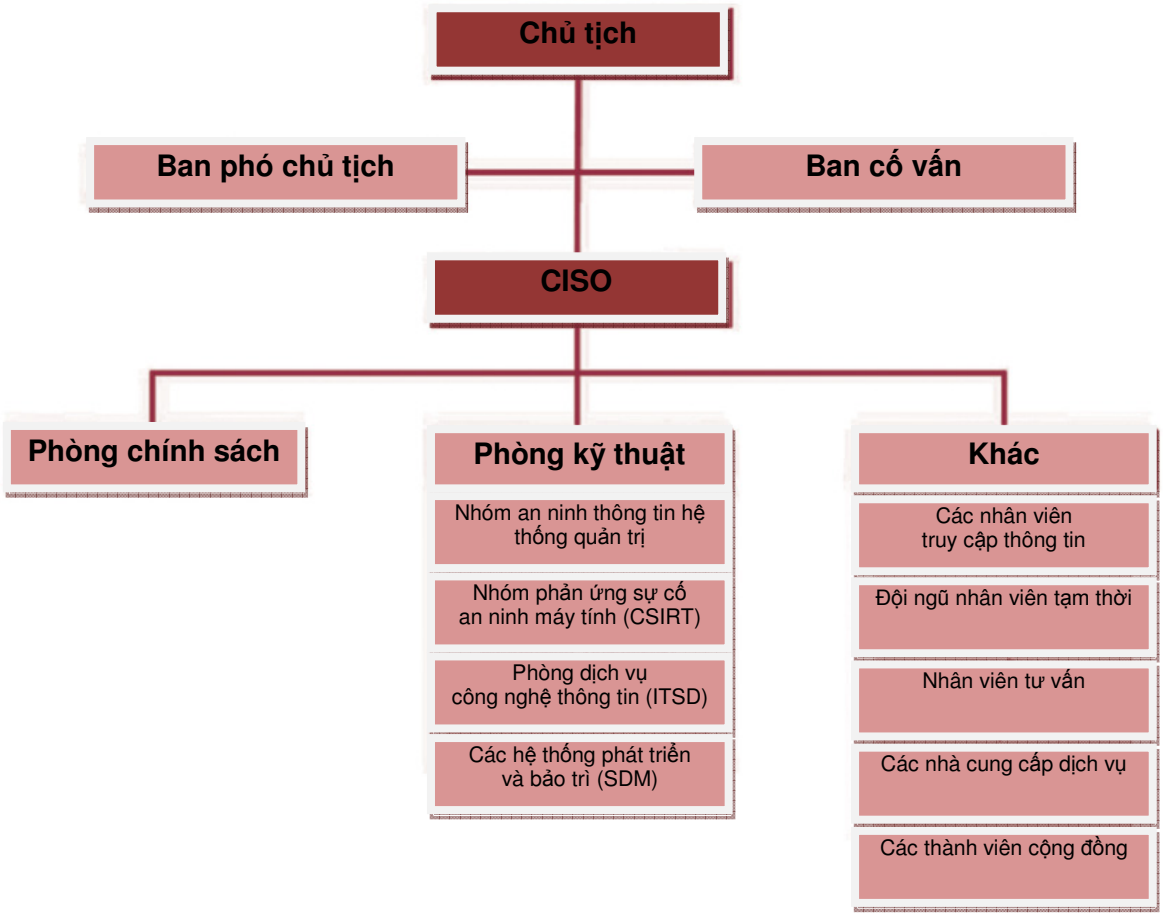
tại chỗ và cung cấp sự hỗ trợ dài hạn. Khu vực tư nhân tham gia vào dự án giai đoạn này, cụ thể là tham gia vào nghiên cứu, phát triển và xây dựng hệ thống.

Việc lập kế hoạch cho khu vực tư nhân tham gia bao gồm các hoạt động nâng cao nhận thức bên cạnh việc xây dựng và tăng cường cơ sở hạ tầng thông tin – truyền thông. Nếu chính phủ nhắm tới khuyến khích khu vực tư nhân chấp nhận chiến lược thông tin, chính phủ cần đóng vai trò hỗ trợ hơn là vai trò điều khiển. Điều này bao gồm việc phân phát các chỉ dẫn an ninh thông tin.

2. Sự thành lập của tổ chức an ninh thông tin, việc xác định các vai trò và trách nhiệm[59]

Một khi định hướng cho chính sách an ninh thông tin đã được đặt ra, việc xây dựng tổ chức cần được tiến hành. Hình 21 cho thấy cấu trúc của một tổ chức an ninh thông tin quốc gia nói chung.

Hình 21. Hình mẫu của tổ chức an ninh thông tin quốc gia



[59] Được trích tại Sinclair Community College, "Information Security Organization - Roles and Responsibilities," http://www.sinclair.edu/about/information/usepolicy/pub/infscply/Information_Security_Organization_-_Roles_and_Responsibilities.htm.

Các tổ chức an ninh thông tin quốc gia thì khác đôi chút tùy theo đặc trưng và văn hóa của mỗi nước. Tuy nhiên, một nguyên tắc cơ bản là đảm bảo rằng các vai trò và trách nhiệm được vạch ra một cách rõ ràng.

Tổ chức quản trị

Ban phó chủ tịch có trách nhiệm chính đối với thông tin được thu thập, duy trì và/hoặc được xác định như là việc tận dụng hay 'sở hữu' bởi từng đơn vị riêng biệt. Họ có thể chỉ định một Cán bộ an ninh thông tin (Information Security Officer) và các cá nhân khác hỗ trợ cho Cán bộ an ninh thông tin trong việc thực thi chính sách an ninh thông tin. Đội ngũ nhân viên được chỉ định này phải đảm bảo rằng những tài sản thông tin trong vòng kiểm soát của họ được định rõ chủ sở hữu, các đánh giá rủi ro được thực hiện, và các quy trình giảm nhẹ đối với những rủi ro đó được thực thi.

Những người giám sát (Giám đốc, Chủ tịch, Người quản lý…) quản lý nhân viên truy cập thông tin và các hệ thống thông tin đồng thời xác định, thi hành và tuân thủ việc kiểm soát an ninh thông tin đối với các lĩnh vực tương ứng của mình. Họ phải đảm bảo rằng tất cả những nhân viên hiểu rõ trách nhiệm các nhân của mình đối với an ninh thông tin đồng thời đảm bảo rằng các nhân viên có quyền truy cập cần thiết để thực hiện công việc của họ. Người giám sát cần định kỳ xem xét tất cả những cấp độ truy cập của người sử dụng nhằm đảm bảo rằng họ thích hợp và có hành động thích hợp để hiệu chỉnh những sự khác biệt cũng như sự thiếu hụt.

Giám đốc an ninh thông tin (Chief Information Security Officer - CISO) có trách nhiệm điều phối và quan sát chính sách an ninh thông tin. Cộng tác một cách chặt chẽ với nhiều phòng ban, CISO có thể khuyến nghị rằng những người giám sát của các phòng ban cụ thể chỉ định người đại diện khác để quan sát và điều phối những yếu tố đặc biệt trong chính sách. CISO cũng trợ giúp những chủ sở hữu thông tin với những thực tiễn an ninh thông tin tốt nhất trong:

- Thiết lập và phổ biến các quy tắc có thể thi hành về tiếp cận và sử dụng hợp lý những tài nguyên thông tin;
- Chỉ đạo/Điều phối việc phân tích và đánh giá rủi ro an ninh thông tin;
- Xây dựng các biện pháp và chỉ dẫn an ninh hợp lý nhằm bảo vệ dữ liệu và các hệ thống;

- Hỗ trợ việc quản lý và giám sát cá khả năng tấn công an ninh hệ thống;
- Chỉ đạo/Điều phối công tác kiểm tra an ninh thông tin; và
- Hỗ trợ việc điều tra/giải quyết các vấn đề và/hoặc những vi phạm đối với an ninh thông tin quốc gia.

Tổ chức kỹ thuật

Nhóm An ninh Thông tin Hệ thống Quản trị (Administrative System Information Security Team) phát triển và thực hiện những biện pháp nhằm đảm bảo rằng việc kiểm soát an ninh ứng dụng quản trị cho phép các bên liên quan khả năng truy cập thích hợp tới thông tin trong khi thỏa mãn luật pháp quốc gia và các nghĩa vụ bảo vệ thông tin phê bình, nhạy cảm và riêng tư. Nhóm phát triển các tiêu chuẩn và quy trình nhằm cung cấp tính sẵn sàng, tính toàn diện và tính tin cẩn của thông tin hệ thống quản trị, bao gồm các quy trình dành cho người dùng yêu cầu đối với truy cập ban đầu và thay đổi quyền truy cập; tài liệu đối với truy cập người dùng được phép, cũng như quyền và nghĩa vụ của người giám sát/người dùng; giải pháp cho các vấn đề cũng như xung đột có liên quan đến an ninh.

Nhóm gồm có Phòng Cán bộ An ninh Thông tin (Division Information Security Officers) và CISO. Nhóm được chỉ dẫn bởi Cục Cán bộ An ninh thông tin và Điều hành viên hệ thống quản trị (Department Information Security Officers and Administrative Systems Administrators).

CSIRT cung cấp thông tin và hỗ trợ các bên liên quan trong việc thực hiện các biện pháp tiên phong nhằm làm giảm rủi ro đối với các sự cố an ninh thông tin, cũng như trong việc kiểm tra, đối phó nhằm giảm thiểu thiệt hại từ những sự cố này khi chúng xảy ra. CSIRT cũng xác định và khuyến nghị các hành động tiếp sau. CSIRT hai lớp bao gồm một nhóm hoạt động phụ trách việc nhận định ban đầu, đối phó, phân loại và xác định những yêu cầu leo thang, và một nhóm quản lý phụ trách việc đi đầu quốc gia trong việc đối phó với những sự cố chính hay quan trọng. CISO và các thành viên đội ngũ IT được ủy thác từ bộ phận Phát triển và Bảo trì các hệ thống, dịch vụ công nghệ thông tin (Information Technology Services and Systems Development and Maintenance) là thành phần của nhóm CSIRT hoạt động. Nhóm quản lý CSIRT bao gồm Phụ trách Thông tin (Chief Information Officer), Phụ trách Giám sát (Chief of Police), Giám đốc Thông tin công (Director of Public Information), Giám đốc Dịch vụ Công nghệ thông tin (Director of Information Technology Services), Giám đốc

Hệ thống phát triển và bảo trì (Director of Systems Development and Maintenance), CISO, nhà quản lý mạng lưới và hệ thống, cố vấn pháp luật, cố vấn nguồn nhân lực, và các đại biểu có chuyên môn kỹ thuật được bổ nhiệm một cách đặc biệt bởi các Phó Chủ tịch.

Các thành viên của **Phòng dịch vụ Công nghệ thông tin (Information Technology Services Department)** bao gồm các kỹ sư và điều hành viên mạng lưới và hệ thống, các nhà cung cấp dịch vụ kỹ thuật như IT Help Desk, các kỹ thuật viên hỗ trợ người dùng, và những nhà quản trị truyền thanh. Họ chịu trách nhiệm đối với việc tích hợp các công cụ an ninh thông tin về mặt kỹ thuật, công tác quản trị cũng như các thực tiễn trong môi trường mạng. Họ tiếp nhận những báo cáo về các sự cố hay thất bại an ninh thông tin được nghi ngờ từ phía người dùng cuối.

Các thành viên **Hệ thống phát triển và bảo trì** bao gồm những nhà phát triển và nhà quản trị cơ sở dữ liệu. Họ phát triển, rén luyện, tích hợp và thực thi các thực tiễn an ninh tốt nhất về các ứng dụng quốc gia, đồng thời đào tạo cho các nhà phát triển ứng dụng Web trong việc sử dụng những nguyên tắc an ninh của ứng dụng.

Các đối tượng khác

Các nhân viên có quyền truy cập thông tin và hệ thống thông tin phải tuân theo những thủ tục và chính sách quốc gia có thể được áp dụng, cũng như bất kỳ các thủ tục hay thực tiễn nào được xây dựng bởi những đơn vị dẫn đầu hay đơn vị định hướng của họ. Điều này bao gồm việc bảo vệ mật mã tài khoản của họ và báo cáo nghi ngờ lạm dụng thông tin hay các sự cố an ninh thông tin cho các bên thích hợp (thông thường là người giám sát của họ).

Đội ngũ nhân viên tạm thời được coi là các nhân viên và có cùng trách nhiệm như một nhân viên toàn thời (full-time) hay bán thời (part-time) chính thức với quyền truy cập tới thông tin và các hệ thống thông tin.

Các nhà tư vấn, nhà cung cấp dịch vụ và các bên tham gia thứ ba khác được cấp quyền truy cập thông tin về một 'nhu cầu nắm bắt' cơ bản. Một tài khoản mạng được yêu cầu bởi một bên thứ ba phải được đưa ra bởi 'người bảo trợ' trong tổ chức mà người đó sẽ đảm bảo rằng người sử dụng bên thứ ba hiểu rõ các trách nhiệm cá nhân có liên quan đến tài khoản mạng, và được chấp thuận bởi giám đốc hay phó chủ tịch thích hợp. Người sử dụng phải giữ bí mật (các) mật khẩu của anh/cô ta đồng thời chịu trách nhiệm đối với bất kỳ hoạt

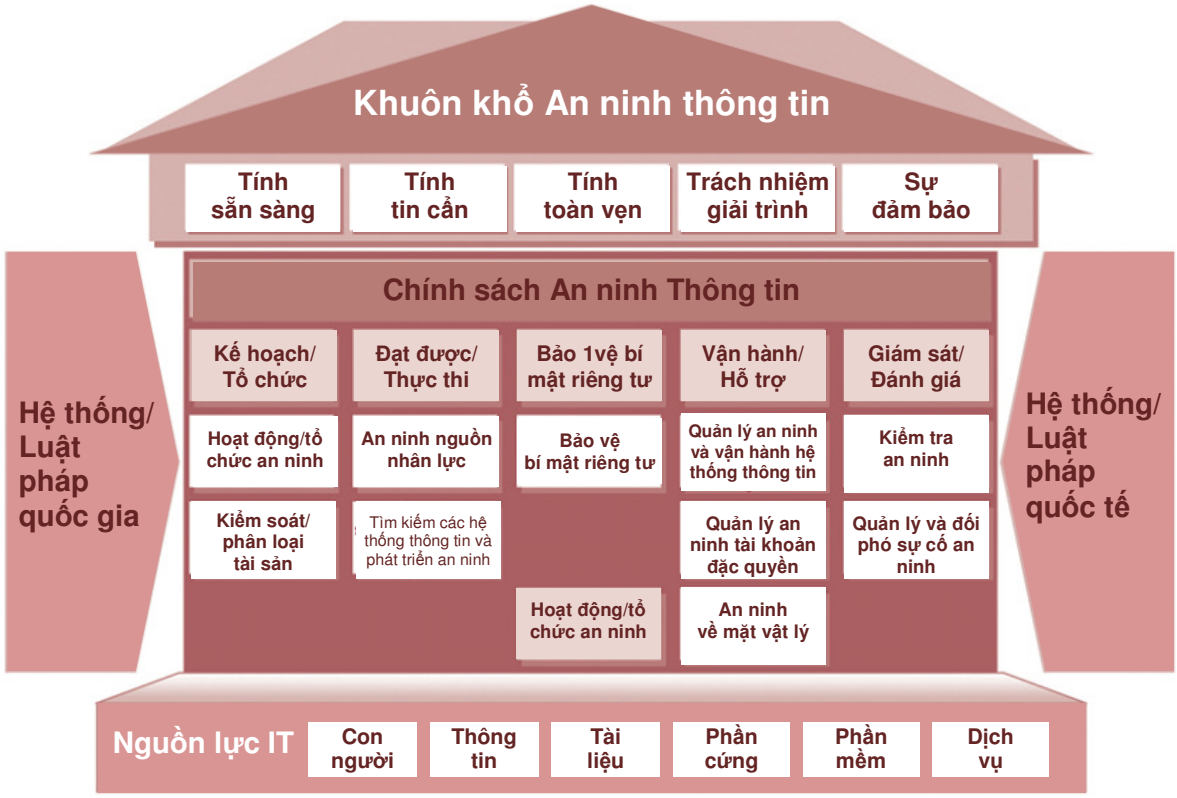
động đưa lại kết quả nào từ việc sử dụng (các) ID của anh/cô ta trong phạm vi kiểm soát hợp lý của anh/cô ta.

3. Thiết lập khuôn khổ cho chính sách an ninh thông tin

Khuôn khổ an ninh thông tin

Khuôn khổ an ninh thông tin đề ra những tham số đối với chính sách an ninh thông tin. Nó đảm bảo rằng chính sách đưa vào các tài nguyên IT (con người, tài liệu thông tin, phần cứng, phần mềm, các dịch vụ); phản ánh các quy tắc và pháp luật quốc tế; và thỏa mãn các nguyên tắc về tính sẵn sàng, tính tin cẩn, tính toàn diện, trách nhiệm giải trình và sự đảm bảo của thông tin. Hình 22 thể hiện một khuôn khổ an ninh thông tin.

Hình 22. Khuôn khổ an ninh thông tin



Chính sách an ninh thông tin là bộ phận quan trọng nhất của khuôn khổ an ninh thông tin. Chính sách bao gồm 5 lĩnh vực, được thảo luận dưới đây.

a. Kế hoạch và tổ chức: Khía cạnh này bao gồm an ninh cho việc vận hành và tổ chức, kiểm soát và phân loại tài sản.

An ninh đối với việc vận hành và tổ chức bao gồm:

- Tổ chức và hệ thống của tổ chức an ninh thông tin quốc gia
- Thủ tục cho mỗi tổ chức an ninh thông tin
- Thiết lập và quản lý an ninh thông tin của quốc gia
- Cộng tác với các cơ quan quốc tế có liên quan
- Cộng tác với một nhóm chuyên gia

Kiểm soát và phân loại tài sản bao gồm:

- Cấp quyền sở hữu và tiêu chuẩn phân loại đối với những tài sản thông tin quan trọng
- Gửi chỉ dẫn và đánh giá rủi ro về những tài sản thông tin quan trọng
- Quản lý các đặc quyền truy cập đối với những tài sản thông tin quan trọng
- Công bố những tài sản thông tin quan trọng
- Đánh giá lại và tận dụng các tài sản thông tin quan trọng
- Quản lý bảo mật tài liệu

b. Thu nhận và thực thi: Khía cạnh này bao gồm an ninh nguồn nhân lực, thu nhận các hệ thống an ninh và phát triển an ninh.

An ninh nguồn nhân lực liên quan đến việc xác định một phương pháp quản lý cho việc thuê mướn nhưng người làm thuê mới, nó bao gồm:

- Các biện pháp đối phó an ninh nguồn nhân lực và đào tạo an ninh
- Xử lý vi phạm các quy định và pháp luật an ninh
- Quản lý an ninh đối với việc truy cập của bên thứ ba
- Quản lý an ninh đối với việc truy cập của các cá nhân thuê ngoài
- Hoạt động và quản lý đối với các bên thứ ba cũng như nhân viên thuê ngoài
- Quản lý an ninh đối với thiết bị và phòng máy tính
- Truy cập tới những công trình và phương tiện chủ yếu
- Xử lý các sự cố an ninh

Thu nhận các hệ thống an ninh và phát triển an ninh bao gồm:

- Kiểm tra an ninh khi một hệ thống thông tin được yêu cầu
- Quản lý an ninh đối với các chương trình ứng dụng bên trong và thuê ngoài
- Một hệ thống mật mã quốc gia (mã hóa chương trình và khóa…)
- Kiểm thử sau khi phát triển chương trình
- Đề xuất các yêu cầu an ninh khi việc thuê ngoài phát triển
- Kiểm tra an ninh trong quá trình phát triển và thu nhận

c. Bảo vệ bí mật riêng tư: Bảo vệ bí mật riêng tư trong một chính sách an ninh thông tin là vấn đề bắt buộc. Tuy nhiên, việc bao hàm nó có một thuận lợi bởi bảo vệ bí mật riêng tư là một vấn đề quốc tế. Cung cấp bảo vệ bí mật riêng tư cần bao hàm các yếu tố sau:

- Thu thập và sử dụng thông tin cá nhân
- Có sự đồng ý trước khi sử dụng bí mật riêng tư của con người
- PIA

d. Hoạt động và hỗ trợ: Khía cạnh này phải tiến hành cùng với an ninh về mặt kỹ thuật và vật lý. Việc sử dụng hệ thống và mạng lưới được quy định chi tiết, đồng thời an ninh về mặt vật lý của cơ sở hạ tầng thông tin và truyền thông được xác định rõ ràng.

Quản lý an ninh và vận hành hệ thống thông tin (Information system operation and security management) liên quan đến việc xác định các vấn đề sau:

- Quản lý an ninh và vận hành máy chủ, mạng lưới, ứng dụng và cơ sở dữ liệu
- Phát triển hệ thống an ninh thông tin
- Ghi chép báo cáo và sao lưu
- Quản lý lưu trữ thông tin
- Tính toán di động
- Tiêu chuẩn cho lưu ký và bảo mật dữ liệu máy tính
- Các dịch vụ thương mại điện tử

Quản lý an ninh tài khoản đặc quyền (Account privilege security management) – Kiểm soát truy cập và quản lý tài khoản được xác định để đảm

bảo tính cẩn mật trong việc sử dụng lưu ký thông tin quốc gia. Điều này bao gồm:

- Quản lý đặc quyền, đăng ký và xóa bỏ của người dùng trong hệ thống thông tin quốc gia
- Quản lý tài khoản và đặc quyền trong mạng lưới được mã hóa

An ninh về mặt vật lý – An ninh về mặt vật lý liên quan đến việc bảo vệ các phương tiện thông tin và truyền thông có chứa những thông tin quan trọng. Nó bao gồm:

- Cấu hình và quản lý các phương pháp an ninh khu vực
- Kiểm soát việc truy cập và truyền tải đối với trung tâm máy tính
- Ngăn ngừa thiệt hại từ những thảm họa tự nhiên và những thảm họa khác

e. Giám sát và đánh giá: Khía cạnh này của chính sách an ninh thông tin đòi hỏi việc xây dựng các tiêu chuẩn và quy trình ngăn chặn những sự cố an ninh cũng như quản lý và đối phó với các sự cố an ninh.

Việc kiểm duyệt an ninh bao gồm:

- Xây dựng một kế hoạch kiểm duyệt an ninh
- Định kỳ thực hiện việc kiểm duyệt an ninh
- Xây dựng/tổ chức các hình thức báo cáo
- Xác định đối tượng của kiểm duyệt an ninh và các mục tiêu báo cáo

Quản lý và đối phó với sự cố an ninh đòi hỏi việc xác định:

- Công việc và vai trò của mỗi tổ chức trong quá trình xử lý các sự cố an ninh
- Các thủ tục đối với việc quan sát và nhận biết những dấu hiệu về sự cố an ninh
- Phương pháp đối phó và thủ tục xử lý sự cố an ninh
- Các biện pháp tiến hành sau khi xử lý sự cố an ninh

4. Xây dựng và/hoặc sửa đổi pháp luật để phù hợp với chính sách an ninh thông tin

Luật pháp phải phù hợp với chính sách an ninh thông tin. Cần có các bộ luật quản lý những cơ quan nhà nước và doanh nghiệp tư nhân. Bảng 14-16 lần lượt liệt kê các bộ luật liên quan đến an ninh thông tin của Nhật Bản, EU và Mỹ. Tại Nhật Bản, đại diện về pháp luật IT là Đạo luật cơ bản về sự hình thành một Xã hội thông tin và Mạng viễn thông tiên tiến (Basic Act on the Formation of an Advanced Information and Telecommunications Network Society). Bộ luật này là tiêu chuẩn cơ bản cho an ninh thông tin của quốc gia và tất cả những vấn đề liên quan đến luật pháp phải tuân theo nó.

Bảng 14. Các bộ luật liên quan đến an ninh thông tin của Nhật Bản

Bộ luật	Lĩnh vực mục tiêu	Mục tiêu điều chỉnh	Hình phạt
Luật truy cập máy tính trái phép (Unauthorized Computer Access Law)	Tất cả các lĩnh vực	Hành động khuyến khích truy cập trái phép và cung cấp thông tin ID của người khác mà không có sự thông báo	
Đạo luật Bảo vệ thông tin cá nhân (Act on the Protection of Personal Information)	Các doanh nghiệp tư nhân sử dụng thông tin riêng tư cho các mục tiêu kinh doanh	Quản lý thông tin bí mật riêng tư (địa chỉ, số điện thoại, e-mail, và các thông tin tương tự)	Trách nhiệm hình sự, phạt tiền
Đạo luật về Chứng thực và Chữ ký điện tử (Act on Electronic Signatures and Certification)		Tạo điều kiện thuận lợi cho thương mại điện tử có được lợi thế trong hoạt động điện tử và Internet thông qua mạng lưới	

Bảng 15. Các bộ luật liên quan đến an ninh thông tin của EU

Bộ luật	Chi tiết
Khuôn khổ điều tiết chung (Chỉ thị 2002/21/EC)	. Đưa ra khuôn khổ điều tiết các dịch vụ và mạng lưới viễn thông . Nhằm bảo vệ bí mật riêng tư thông qua các mạng truyền thông an toàn
Chỉ thị EU về Bảo vệ dữ liệu (Chỉ thị 1995/46/EC)	. Hướng dẫn về việc xử lý và tự do loại bỏ thông tin cá nhân . Pháp luật cơ bản xác định trách nhiệm của các quốc gia thành viên và công nhận quyền tối thượng của các cá nhân đối với thông tin riêng tư . Nghiêm ngặt hơn tiêu chuẩn của Mỹ
Chỉ thị EU về Chữ ký điện tử (Chỉ thị 1999/93/EC) Chỉ thị EU về Thương mại điện tử (Chỉ thị 2000/31/EC)	. Quản lý việc sử dụng chữ ký điện tử . Điều chỉnh việc thực hiện thương mại điện tử
Hiệp ước về tội phạm mạng	. Hiệp ước quốc tế toàn diện nhất về tội phạm mạng . Xác định chi tiết tất cả những hành động phạm tội có sử dụng Internet và những hình phạt tương ứng
Hướng dẫn Bảo quản dữ liệu Truyền thông và Mạng lưới	. Yêu cầu các nhà cung cấp dịch vụ truyền thông lưu giữ dữ liệu cuộc gọi từ 6 – 24 tháng (được ban hành sau các cuộc tấn công khủng bố tại Madrid và London năm 2004 và 2005)

Bảng 16. Các bộ luật liên quan đến an ninh thông tin của Mỹ

Bộ luật	Lĩnh vực mục tiêu	Mục tiêu điều chỉnh	Hình phạt
Luật Quản lý An ninh thông tin Liên bang năm 2002	Các cơ quan hành chính Liên bang	Thông tin của các cơ quan hành chính, hệ thống IT, chương trình an ninh thông tin	-

Luật Trách Lợi Bảo hiểm Y tế năm 1996	Các tổ chức y tế và các nhà cung cấp dịch vụ y tế	Dữ liệu điện tử về thông tin y tế cá nhân	Trách nhiệm hình sự, phạt tiền
Luật Gramm-Leach-Bliley năm 1999	Các tổ chức tài chính	Thông tin bí mật riêng tư của các khách hàng	Trách nhiệm hình sự, phạt tiền
Luật Sarbanes-Oxley năm 2002	Liệt kê các công ty trên Thị trường chứng khoán Mỹ	Kiểm soát nội bộ và công khai các bản ghi tài chính	Trách nhiệm hình sự, phạt tiền
Luật Thông tin vi phạm an ninh cơ sở dữ liệu California năm 2003	Các cơ quan hành chính và doanh nghiệp tư nhân tại California	Thông tin bí mật riêng tư được mã hóa	Phạt tiền và thông báo tới người bị hại

5. Phân bổ một nguồn ngân sách cho việc thực hiện chính sách thông tin

Việc thực hiện một chính sách đòi hỏi có nguồn ngân sách. Bảng 17 cho biết ngân sách dành cho an ninh thông tin tại Nhật Bản và Mỹ trong vài năm gần đây.

Bảng 17. Ngân sách bảo vệ thông tin của Nhật và Mỹ

Nhật Bản	**2004**	**2005**
Tổng ngân sách hàng năm	JPY 848,967,000,000,000	JPY 855,195,000,000,000
Ngân sách dành cho an ninh thông tin	JPY 267,000,000,000	JPY 288,000,000,000
Tỉ lệ trong tổng ngân sách	0.03%	0.03%
Mỹ	**2006**	**2007**
Tổng ngân sách hàng năm	USD 2,709,000,000,000	USD 2,770,000,000,000
Ngân sách dành cho an ninh thông tin	USD 5,512,000,000	USD 5,759,000,000
Tỉ lệ trong tổng ngân sách	0.203%	0.208%

Bài tập

Nếu đất nước bạn có một chính sách an ninh thông tin, hãy phác họa sự phát triển của nó theo 5 khía cạnh của quá trình xây dựng chính sách an ninh thông tin được mô tả ở trên. Nghĩa là mô tả về:

1. Định hướng chính sách
2. Tổ chức an ninh thông tin
3. Khuôn khổ chính sách
4. Các pháp luật hỗ trợ cho chính sách an ninh thông tin
5. Phân bổ ngân sách cho an ninh thông tin

Nếu đất nước bạn chưa có một chính sách an ninh thông tin nào, hãy chỉ ra một số triển vọng đối với mỗi một trong số 5 khía cạnh ở trên hướng tới việc xây dựng chính sách. Sử dụng những câu hỏi sau đây như là gợi ý:

1. Điều gì sẽ là định hướng cho chính sách an ninh thông tin của đất nước bạn?
2. Cái gì được đưa ra trong việc thiết lập tổ chức? Những tổ chức nào sẽ liên quan đến việc phát triển và thực thi chính sách an ninh thông tin ở đất nước bạn?
3. Những vấn đề cụ thể của khuôn khổ chính sách là gì?
4. Những luật pháp nào cần được ban hành và/hoặc bị bãi bỏ để hỗ trợ cho chính sách thông tin?
5. Những cân nhắc về tài chính nào sẽ được đưa vào bản kê? Trong trường hợp nào ngân sách được rút ra?

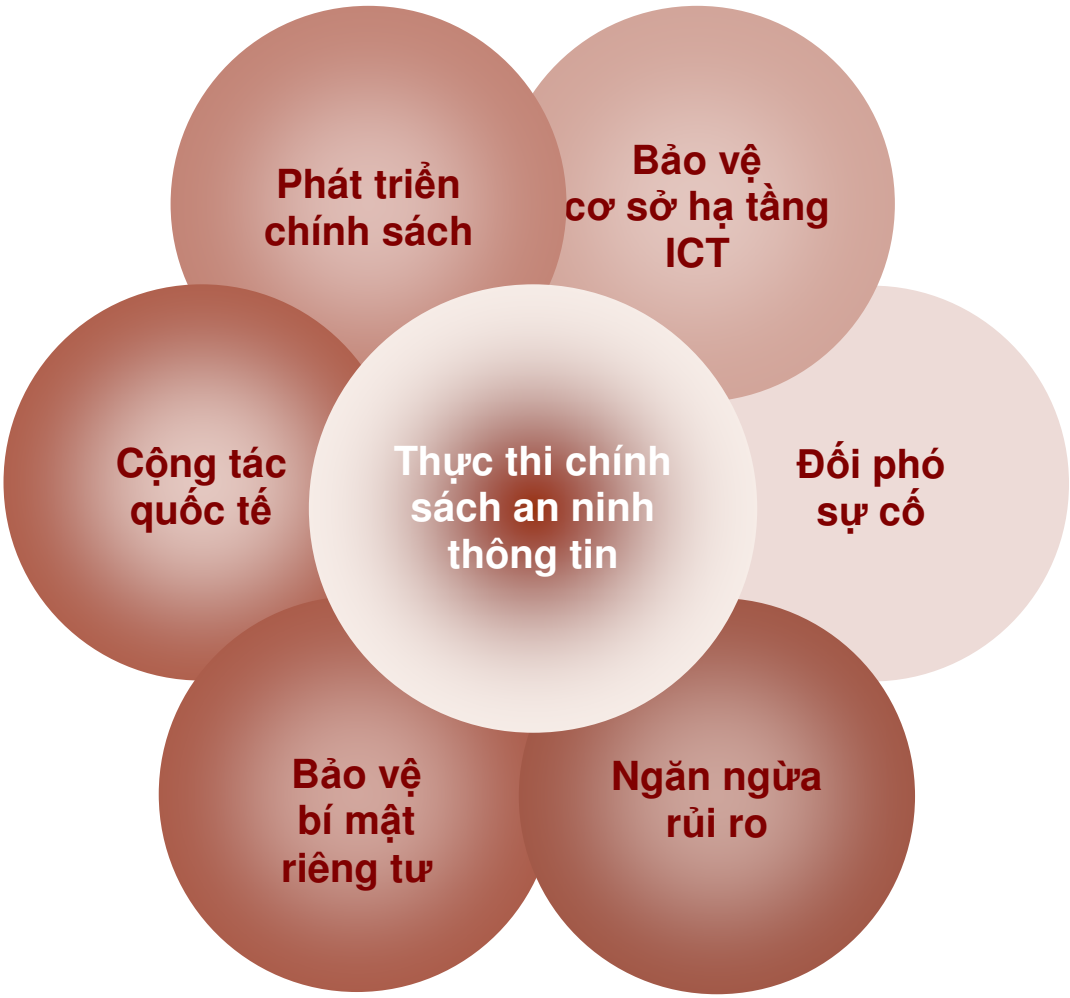
Những người tham gia khóa học đến từ cùng một quốc gia có thể cùng nhau thực hiện bài tập này.

7.3. Thực hiện/thực thi chính sách

Việc thực thi suôn sẻ chính sách an ninh thông tin đòi hỏi sự cộng tác giữa chính phủ, tư nhân và các tổ chức quốc tế. Hình 23 cho thấy những lĩnh vực

cụ thể của việc thực thi chính sách thông tin, nơi mà sự công tác là yếu tố quyết định.

Hình 23. Các lĩnh vực công tác trong việc thực thi chính sách an ninh thông tin



Phát triển chính sách an ninh thông tin

Bảng 18 cho biết chính phủ, khu vực tư nhân, và các tổ chức quốc tế có thể đóng góp vào việc phát triển chính sách an ninh thông tin quốc gia như thế nào.

Bảng 18. Ví dụ về cộng tác trong việc phát triển chính sách an ninh thông tin

Khu vực	Đóng góp vào việc phát triển chính sách
Chính phủ	. Chiến lược quốc gia và tổ chức hoạch định: đảm bảo phù hợp giữa chính sách thông tin và kế hoạch quốc gia

	. Tổ chức công nghệ thông tin và truyền thông: đảm bảo sự điều phối trong việc xây dựng tiêu chuẩn công nghệ an ninh thông tin của quốc gia . Tổ chức phân tích xu hướng an ninh thông tin: phản ánh xu hướng an ninh trong nước và quốc tế đồng thời phân tích về chính sách . Tổ chức phân tích chính sách: kiểm tra sự phù hợp giữa chính sách an ninh thông tin và những luật pháp hiện tại . Tổ chức thông tin quốc gia: cộng tác trong việc thiết lập định hướng và xây dựng chiến lược . Các cơ quan điều tra: công tác trong việc xử lý những sự cố an ninh
Tư nhân	. Các công ty tư vấn an ninh thông tin: sử dụng những đơn vị chuyên nghiệp trong việc hoạch định chính sách an ninh thông tin . Phòng thí nghiệm công nghệ an ninh thông tin tư nhân: xây dựng các tiêu chuẩn công nghệ liên quan đến an ninh thông tin . Phòng an ninh thông tin của các trường đại học và/hoặc các trường cao học: đưa ra ý kiến chuyên môn về việc xây dựng chính sách
Các tổ chức quốc tế	. Đảm bảo tuân thủ các tiêu chuẩn chính sách quốc tế . Điều phối đối phó với những sự cố và các mối đe dọa quốc tế

Quản lý và bảo vệ cơ sở hạ tầng thông tin, truyền thông

Sử dụng hiệu quả (thu thập, lưu ký, v.v…) thông tin đòi hỏi việc bảo vệ và quản trị thích hợp đối với cơ sở hạ tầng IT. Một chính sách an ninh thông tin tốt sẽ vô nghĩa nếu thiếu một cơ sở hạ tầng IT lành mạnh.

Quản lý và bảo vệ hiệu quả cơ sở hạ tầng thông tin và truyền thông yêu cầu sự hợp tác giữa các nhà quản lý lĩnh vực mạng lưới, hệ thống và IT. Một điều cũng mang lại lợi ích đó là sự hợp tác giữa các tổ chức công và tư nhân (Bảng 19).

Bảng 19. Ví dụ về hợp tác trong việc quản lý và bảo vệ cơ sở hạ tầng thông tin, truyền thông

Khu vực	Đóng góp vào việc quản lý và bảo vệ Cơ sở hạ tầng thông tin và truyền thông
Chính phủ	. Mạng lưới thông tin và truyền thông có liên quan đến tổ chức: xác định thành phần kết cấu và mức độ an ninh của mạng lưới thông tin

	và truyền thông quốc gia . Phòng thí nghiệm công nghệ thông tin và truyền thông: đưa ra các tiêu chuẩn chung và chấp nhận công nghệ có thể sử dụng
Tư nhân	. Các nhà cung cấp ISP: hợp tác trong thành phần của mạng lưới thông tin và truyền thông quốc gia . Phòng thí nghiệm công nghệ thông tin và truyền thông: cung cấp các dịch vụ phát triển kỹ thuật đồng thời hợp tác trong việc vận hành công nghệ an ninh và một cơ sơ hạ tầng thông tin và truyền thông ổn định
Các tổ chức quốc tế	. Hợp tác với tổ chức tiêu chuẩn công nghệ quốc tế cho thông tin và truyền thông, và cho việc bảo mật công nghệ thông tin mới

Ngăn ngừa và đối phó với các sự cố, mối đe dọa

Đối phó một cách hiệu quả các mối đe dọa và sự vi phạm an ninh thông tin đòi hỏi sự hợp tác giữa tổ chức thông tin quốc gia, các cơ quan điều tra và các tổ chức pháp lý, cũng như các tổ chức chỉ đạo kiểm soát sự cố an ninh và đánh giá thiệt hại. Nó cũng cần hợp tác với tổ chức có thể phân tích những khả năng bị tấn công về mặt kỹ thuật và đưa ra các biện pháp đối phó về mặt kỹ thuật.

Bảng 20. Ví dụ về hợp tác trong việc đối phó sự cố an ninh thông tin

Khu vực	Sự đóng góp
Các tổ chức Chính phủ	. Tổ chức đối phó sự cố an ninh: đưa ra phân tích tình huống, đối phó sự cố thâm nhập trái phép, và công nghệ để đối phó với những vi phạm và các sự cố . Tổ chức thông tin quốc gia: phân tích và kiểm tra các sự cố và những vi phạm liên quan đến an ninh thông tin . Các cơ quan điều tra: hợp tác với tổ chức có liên quan trong việc tóm bắt và truy tố kẻ phạm tội . Tổ chức cung cấp đánh giá về an ninh: kiểm tra sự an toàn và tính tin cậy mạng lưới thông tin và sản phẩm an ninh thông tin . Tổ chức giáo dục an ninh thông tin: phân tích nguyên nhân của các sự cố an ninh thông tin đồng thời rèn luyện học viên để ngăn chặn sự tái diễn của các rủi ro
Các nhóm Tư	. Tổ chức đối phó sự cố tư nhân: đưa ra sự đối phó và hỗ trợ về mặt

nhân	kỹ thuật . Các cơ quan điều tra tư nhân: hợp tác cùng với các cơ quan điều tra của quốc gia
Các tổ chức quốc tế	. Trong trường hợp những sự cố và các mối đe dọa trên phạm vi quốc tê, báo cáo và hợp tác với Interpol, CERT/CC

Ngăn ngừa các sự cố an ninh thông tin

Việc ngăn ngừa các sự cố và vi phạm an ninh thông tin bao gồm công tác giám sát, giáo dục và quản lý sự thay đổi. CSIRT quốc gia là đơn vị giám sát chủ đạo. Một khu vực quan trọng thì có chính sách thông tin và dữ liệu giám sát thực tế tương xứng. Do vậy, cần thiết phải thảo luận về phạm vi của việc giám sát chính sách thông tin. Hơn nữa, điều này quan trọng đối với giáo dục các nhân viên trong khu vực tư nhân và chính phủ, cũng như khu vực công cộng nói chung về chính sách an ninh thông tin. Nó cũng có thể cần thiết để thay đổi các quan điểm nào đó về thông tin và hành vi tác động tới an ninh thông tin. Giáo dục về an ninh thông tin và quản lý sự thay đổi được chỉ rõ trong US SP 800-16 (Những Yêu cầu Đào tạo đối với An ninh Công nghệ Thông tin - Information Technology Security Training Requirements).

Bảng 21. Ví dụ về hợp tác trong việc ngăn ngừa sự cố và vi phạm đến anh ninh thông tin

Khu vực	Sự điều phối
Các tổ chức Chính phủ	. Cơ quan giám sát: không ngừng giám sát mạng lưới và dò tìm nâng cao đối với những mối đe dọa an ninh . Cơ quan thu thập: chia sẻ thông tin với các tổ chức quốc tế và những cơ quan an ninh . Đơn vị đào tạo: thực hiện đào tạo mô phỏng định kỳ nhằm phát triển khả năng và năng lực đối phó một cách nhanh chóng với những sự cố và vi phạm tới an ninh thông tin
Các tổ chức tư nhân	. Các nhà cung cấp ISP, công ty xử lý virus và kiểm soát an ninh: cung cấp thực trạng lưu lượng, thông tin về các loại hình tấn công và các mô tả về sâu/virus
Các tổ chức quốc tế	. Cung cấp thông tin về các loại hình tấn công, những mô tả về sâu/virus và các vấn đề tương tự

An toàn bí mật riêng tư

Sự hợp tác là cần thiết để xây dựng các biện pháp bảo vệ bí mật riêng tư trên Internet, ngăn chặn sự cố thông tin về địa điểm của cá nhân, bảo vệ các báo cáo và thông tin về sinh vật học của cá nhân trước những xâm phạm về bí mật riêng tư.

Bảng 22. Ví dụ về hợp tác trong bảo vệ bí mật riêng tư

Khu vực	Sự điều phối
Các cơ quan Chính phủ	. Tổ chức phân tích hệ thống: chỉ đạo các hoạt động liên quan đến thông tin về địa điểm của cá nhân, và phân tích những xu hướng bên trong và bên ngoài của việc bảo vệ thông tin cá nhân . Tổ chức hoạch định: cải thiện các hệ thống/luật pháp, các biện pháp kỹ thuật/quản trị và quản lý các tiêu chuẩn . Hỗ trợ kỹ thuật: phối hợp xác nhận người sử dụng mạng cho các doanh nghiệp . Các tổ chức dịch vụ: điều phối hỗ trợ cho việc xử lí các sự cố thư rác và vi phạm bí mật riêng tư
Các tổ chức tư nhân	. Tổ chức an ninh thông tin tư nhân: đăng ký các yêu cầu và thiết lập các hiệp hội hợp tác về an ninh thông tin cá nhân . Cố vấn an ninh thông tin cá nhân
Các tổ chức quốc tế	. Hợp tác nhằm áp dụng những tiêu chuẩn an ninh thông tin cá nhân trên phạm vi quốc tế

Điều phối quốc tế

An ninh thông tin không thể đạt được bằng những nỗ lực của một quốc gia đơn lẻ bởi các vi phạm về an ninh thông tin có xu hướng diễn ra trên phạm vi toàn cầu. Do đó, vấn đề điều phối quốc tế trong việc bảo vệ an ninh thông tin, cả trong khu vực chính phủ và khu vực tư nhân, cần được thể chế hóa.

Đối với khu vực tư nhân, tổ chức quốc tế có liên quan đến việc thúc đẩy và bảo vệ an ninh thông tin là CERT/CC. Các chính phủ, ENISA (đối với EU) và ITU hướng tới mục đích hợp tác về an ninh thông tin giữa các quốc gia.

Tại mỗi quốc gia, cần phải có một cơ quan chính phủ có vai trò tạo điều kiện hợp tác thuận lợi cho cả các tổ chức chính phủ lẫn tư nhân với những cơ quan, tổ chức quốc tế.

Bài tập

1. Xác định các cơ quan chính phủ và những tổ chức tư nhân tại đất nước bạn mà cần thiết hợp tác và cộng tác trong việc thực thi một chính sách an ninh thông tin quốc gia. Đồng thời xác định những tổ chức quốc tế có nhu cầu hợp tác về vấn đề này.
2. Đối với mỗi lĩnh vực của hợp tác trong việc thực thi chính sách thông tin được thể hiện ở hình 23, xác định những hoạt động hay hành động cụ thể mà các cơ quan hay tổ chức này có thể tiến hành

Những học viên cùng đến từ một quốc gia có thể thực hiện bài tập này cùng nhau.

7.4. Xem xét lại và đánh giá Chính sách an ninh thông tin

Bước cuối cùng trong việc hoạch định chính sách an ninh thông tin và bổ sung những khía cạnh chưa hoàn thiện. Việc sửa đổi chính sách là cần thiết sau khi hiệu quả của một chính sách an ninh thông tin được xác định.

Một phương pháp đánh giá chính sách trong nước có thể được thực hiện để xác định hiệu quả của chính sách an ninh thông tin quốc gia. Các khía cạnh của phương pháp này được thảo luận dưới đây.

Sử dụng các tổ chức kiểm tra

Có những tổ chức có vai trò tiến hành đánh giá và xem xét chính sách. Như vậy một tổ chức cần tiến hành kiểm tra thường xuyên chính sách an ninh thông tin quốc gia. Ngoài ra, tổ chức này cũng cần độc lập với tổ chức hoạch định chính sách an ninh thông tin và tổ chức thực thi.

Sửa đổi chính sách an ninh thông tin

Các khía cạnh có vấn đề thường được nhận diện trong suốt quá trình kiểm tra. Cần có một quy trình sửa đổi chính sách để xử lý các vấn đề này.

Những thay đổi về môi trường

Điều quan trọng là cần phản ứng một cách nhanh nhạy trước những thay đổi của môi trường chính sách. Những thay đổi nảy sinh từ các khả năng bị tấn công và các mối đe dọa (các cuộc tấn công) quốc tế, thay đổi cơ sở hạ tầng IT, thay đổi mức độ của thông tin thiết yếu, và những thay đổi quan trọng khác cần được lập tức phản ánh trong chính sách an ninh thông tin quốc gia.

Tự kiểm tra

1. Các giai đoạn khác nhau trong chu kỳ sống của chính sách an ninh thông tin tác động lẫn nhau như thế nào? Bạn có thể bỏ qua giai đoạn nào? Tại sao có hoặc tại sao không?
2. Tại sao sự hợp tác giữa rất nhiều khu vực lại quan trọng trong quá trình phát triển và thực thi chính sách an ninh thông tin?

PHỤ LỤC

Tài liệu đọc thêm

Butt, Danny, ed. 2005. *Internet Governance: Asia-Pacific Perspectives*. Bangkok: UNDP-APDIP. http://www.apdip.net/publications/ict4d/igovperspectives.pdf.

CERT. CSIRT FAQ. Carnegie Mellon University. http://www.cert.org/csirts/csirt_faq.html.

CERT. Security of the Internet. Carnegie Mellon University. http://www.cert.org/encyc_article/tocencyc.html.

Dorey, Paul and Simon Perry, ed. 2006. *The PSG Vision for ENISA*. Permanent Stakeholders Group. http://www.enisa.europa.eu/doc/pdf/news/psgvisionforenisafinaladoptedmay2006 version.pdf.

ESCAP. Module 3: Cyber Crime and Security. http://www.unescap.org/icstd/POLICY/ publications/internet- use- for-business-evelopment/module3-sources.asp.

Europa. Strategy for a secure information society (2006 communication). European Commission. http://europa.eu/scadplus/leg/en/lvb/l24153a.htm.

Information and Privacy Office. 2001. *Privacy Impact Assessment: A User's Guide*. Ontario: Management Board Secretariat. http://www.accessandprivacy.gov.on.ca/english/pia/pia1.pdf.

Information Security Policy Council. *The First National Strategy on Information Security*. 2 February 2006. http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf.

ISO. ISO/IEC27001:2005. http://www.iso.org/iso/iso_catalogue/catalogue_tc/ catalogue_detail.htm?csnumber=42103.

ITU and UNCTAD. 2007. Challenges to building a safe and secure Information Society. In *World Information Society Report 2007*, 82-101. Geneva: ITU. http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/report.html.

ITU-D Applications and Cybersecurity Division. ITU National Cybersecurity / CIIP Self-Assessment Tool. ITU. http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html.

Killcrece, Georgia. 2004. *Steps for Creating National CSIRTs*. Pittsburgh: Carnegie Mellon University. http://www.cert.org/archive/pdf/NationalCSIRTs.pdf.

Killcrece, Georgia, Klaus-Peter Kossakowski, Robin Ruefle and Mark Zajicek. 2003. *Organizational Models for Computer Security Incident Response Teams (CSIRTs)*. Pittsburgh: Carnegie Mellon University. http://www.cert.org/archive/pdf/03hb001.pdf.

OECD. 2002. *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. Paris: OECD. http://www.oecd.org/dataoecd/16/22/15582260.pdf.

OECD. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

Shimeall, Tim and Phil Williams. 2002. *Models of Information Security Trend Analysis*. Pittsburgh: CERT Analysis Center. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.11.8034.

The White House. 2003. *The National Strategy to Secure Cyberspace*. Washington, D.C.: The White House. http://www.whitehouse.gov/pcipb.

Các lưu ý đối với Giảng viên

Như đã lưu ý trong phần "Về Chuỗi học phần", học phần này cũng như các học phần khác trong chuỗi được thiết kế để mang lại giá trị cho nhiều nhóm học viên khác nhau và trong các điều kiện quốc gia biến đổi, thay đổi. Các học phần cũng được thiết kế để có thể trình bày, toàn bộ hay một phần, bằng nhiều hình thức khác nhau, trực tuyến (on-line) hay ngoại tuyến (off-line). Các học phần cũng có thể nghiên cứu độc lập hoặc theo nhóm trong các đơn vị đào tạo cũng như trong các cơ quan chính phủ. Nền tảng của người tham gia cũng như độ dài của các buổi học sẽ xác định mức độ chi tiết trong các nội dung trình bày.

Những "lưu ý" này mang lại cho các giảng viên một số ý kiến và đề xuất để việc trình bày nội dung học phần hiệu quả hơn. Chỉ dẫn sâu hơn về các phương pháp cận và chiến lược đào tạo được đưa ra trong cẩm nang hướng dẫn về kế hoạch giảng dạy được xây dựng như một tài liệu hướng dẫn cho chuỗi học phần của *Bộ giáo trình những kiến thức cơ bản về công nghệ thông tin và truyền thông cho lãnh đạo trong cơ quan nhà nước*. Cẩm nang này có thể tìm thấy tại địa chỉ: http://www.unapcict.org/academy.

Cấu trúc các buổi học

Với một buổi học 90 phút

Đưa ra cái nhìn tổng quan về những khái niệm cơ bản và các nguyên tắc/tiêu chuẩn quốc tế của an ninh thông tin và bảo vệ bí mật riêng tư (Chương 1 và Chương 5 của học phần). Nhấn mạnh sự cần thiết về chính sách bảo vệ bí mật riêng tư và an ninh thông tin có hiệu quả, phù hợp.

Với một buổi học 3 tiếng

Phân chia buổi học thành hai phần. Trong phần đầu, tập trung vào những khái niệm và xu hướng cơ bản trong an ninh thông tin, bao gồm sự phân tích xu hướng đe dọa đối với an ninh thông tin (Chương 2). Trong phần thứ hai, tập trung vào các khái niệm cơ bản và nguyên tắc bảo vệ bí mật riêng tư, tạo điều kiện cho một buổi thảo luận về những vấn đề tác động đến bảo vệ bí mật riêng tư và đánh giá ngắn gọn tác động bí mật riêng tư.

Với một buổi học kéo dài cả ngày (6 tiếng)

Sau khi có cái nhìn tổng quan về các khái niệm và nguyên tắc cơ bản về an ninh thông tin và bảo vệ bí mật riêng tư, tập trung vào việc phát triển và thực thi chính sách an ninh thông tin (Chương 7). Bạn có thể bắt đầu bằng việc hỏi các học viên về chính sách có liên quan đến an ninh thông tin và bảo vệ bí mật riêng tư. Sau đó trình bày ngắn gọn vòng đời của chính sách an ninh thông tin trước khi đi vào quy trình xây dựng chính sách. Các học viên đến từ nhiều quốc gia khác nhau với một chính sách an ninh thông tin có thể được yêu cầu đánh giá chính sách đó theo những nguyên tắc và quy trình đã thảo luận, trong khi những học viên đến từ các quốc gia không có một chính sách an ninh thông tin nào có thể được yêu cầu phác họa một số khía cạnh của chính sách (xem hoạt động học tập tại cuối phần 7.2).

Với một buổi học kéo dài 2 ngày

Ngày đầu tiên có thể tiến hành như mô tả ở trên, ngày thứ hai có thể tập trung vào phương pháp và các hoạt động an ninh thông tin (Chương 3 và 4), đặc biệt là việc xây dựng CSIRT (Chương 6). Những ví dụ từ các quốc gia khác nhau có thể được chia ra, và nên khuyến khích học viên xác định mô hình CSIRT phù hợp nhất để thiết kế các cơ chế can thiệp an ninh cụ thể cho bối cảnh đất nước mình.

Tính tương tác

Điều quan trọng là người học có được tính tương tác và những bài học thực tiễn. Học phần cung cấp rất nhiều thông tin có ích, tuy nhiên các học viên cần có khả năng phân tích thông tin này và áp dụng chúng tại nơi mà chúng có ích. Một số trường hợp nghiên cứu được đưa ra trong học phần, bất cứ khi nào có thể, chúng có thể được thảo luận dưới dạng các nguyên tắc và khái niệm an ninh thông tin. Tuy nhiên, học viên cũng cần được khuyến khích để tìm hiểu những vấn đề xác thực và những vấn đề về bảo vệ bí mật riêng tư và an ninh thông tin trong bối cảnh riêng của họ.

Về KISA

Cơ quan an ninh thông tin Hàn Quốc (Korea Information Security Agency - KISA) được chính phủ thành lập năm 1996 như là một trung tâm chiu trách nhiệm xúc tiến hoạt động hoạch định chính sách hiệu quả trên phạm vi toàn quốc nhằm nâng cao an ninh thông tin. Các chức năng của nó gồm có ngăn ngừa và đối phó với những xâm phạm Internet, đối phó thư rác, bảo vệ bí mật riêng tư, chữ ký điện tử, bảo vệ cơ sở hạ tầng thiết yếu, đánh giá an ninh của các sản phẩm an ninh thông tin, phát triển công nghệ và chính sách chuyên sâu, và nâng cao nhận thức đối với việc thiết lập một xã hội thông tin an toàn và tin cậy.

UN-APCICT

Trung tâm đào tạo công nghệ thông tin và truyền thông phục vụ phát triển Châu Á Thái Bình Dương (UN-APCICT) là một đơn vị thành viên của Ủy ban Kinh tế Xã hội Liên hợp quốc trong khu vực Châu Á và Thái Bình Dương (ESCAP). UN-APCICT hướng tới tăng cường nỗ lực của các quốc gia thành viên ESCAP nhằm sử dụng ICT trong quá trình phát triển kinh tế xã hội của họ thông qua xây dựng năng lực con người và các cơ quan. Hoạt động của UN-APCICT tập trung vào các lĩnh vực:

- Đào tạo: nâng cao kiến thức và kỹ năng ICT cho các nhà hoạch định chính sách và chuyên gia ICT, đồng thời tăng cường năng lực của đội ngũ giảng viên ICT và các tổ chức đào tạo ICT;
- Nghiên cứu: thực hiện các nghiên cứu phân tích liên quan đến phát triển nguồn nhân lực trong lĩnh vực ICT; và
- Tư vấn: cung cấp dịch vụ tư vấn về các chương trình phát triển nguồn nhân lực tới các thành viên của ESCAP và các thành viên cộng tác.

UN-APCICT đặt trụ sở tại Incheon, Hàn Quốc

http://www.unapcict.org

ESCAP

ESCAP là một nhánh phát triển khu vực của Liên hợp quốc và hoạt động như trung tâm phát triển kinh tế xã hội chính của Liên hợp quốc ở Châu Á và Thái Bình Dương. Nhiệm vụ của ESCAP là thúc đẩy sự hợp tác giữa 53 thành viên và 9 thành viên công tác. ESCAP đưa ra những liên kết mang tính chiến lược giữa các chương trình và vấn đề cấp toàn cầu và quốc gia. Nó hỗ trợ chính phủ của các nước trong khu vực trong việc củng cố vị trí và ủng hộ hướng đi của khu vực để chuẩn bị cho những thách thức kinh tế xã hội trong điều quá trình toàn cầu hóa thế giới. Văn phòng ESCAP đặt tại Bangkok, Thái Lan.

http://www.unesscap.org