**http://www.quantrimang.com.vn/xay-dung-he-thong-isms-chung-chi-iso-27001-77640**

**Làm sao có được một hệ thống công nghệ thông tin (CNTT) an ninh, an toàn? Làm sao để minh chứng rằng hệ thống của ta là đáng tin cậy? Đó là những câu hỏi mà tôi trăn trở khi thực hiện nhiệm vụ quản trị mạng của mình.**Để trả lời câu hỏi đó, tôi đã làm quen với khá nhiều các tài liệu, văn bản khác nhau như hệ thống ISMS, BS7799, ISO/IEC17799, ISO27001, ISO27002,…

Đọc, hiểu, thấm nhuần những văn bản này với tôi thực sự vất vả mà cũng chưa chắc là mình đã hiểu đúng chưa, hiểu hết chưa. Đến nay, tôi lại phải chịu trách nhiệm triển khai hệ thống ISMS trong đơn vị mình. Trong "mớ bòng bong " này, tôi đã cố gắng tìm hiểu và "ngộ" ra được một số điều, nên cảm thấy bức tranh trở nên có trật tự hơn. Tôi viết mấy dòng này để miêu tả lại quá trình "debug" của mình với hy vọng nó có thể hữu ích cho ai đó đang ở trong hoàn cảnh như tôi.

Information Security Management System, hay ISMS, có thể hiểu là một bộ qui định (như chính sách, qui trình, hướng dẫn, biểu mẫu…) được thực hiện trong một tổ chức (doanh nghiệp, trường học) để đảm bảo hệ thống thông tin của tổ chức được an ninh, an toàn một cách phù hợp với mục tiêu kinh doanh của tổ chức. Tôi nghĩ rằng phát biểu trên là chính xác, nhưng còn rất trừu tượng, còn nhiều điều không rõ ràng về ISMS. Mổ xẻ, giải thích phát biểu trên là nội dung cơ bản của phần sau.

Lý do chính để tồn tại của doanh nghiệp là kinh doanh để phát triển tài sản (asset). Vì vậy, có thể nói, tài sản là nền tảng của doanh nghiệp. Điều phức tạp là tài sản hiện nay rất phong phú và tồn tại dưới nhiều dạng khác nhau. Người ta có thể phân ra 6 loại hình thức tồn tại của tài sản khác nhau là:

- Thông tin số  
- Giấy tờ tài liệu  
- Phần mềm  
- Phần cứng/vật lý  
- Con người  
- Các dịch vụ bổ sung

Với việc phân loại tài sản thành 6 loại, chúng ta có thể dễ dàng hơn trong việc khởi đầu công tác xây dựng ISMS là liệt kê và định giá tất cả các tài sản của doanh nghiệp.

**Liệt kê tài sản.** Đây là một công việc không quá khó vì chúng ta có thể căn cứ vào danh sách trang thiết bị phần cứng, phần mềm, danh sách các loại văn bản phát sinh trong quá trình hoạt động của tổ chức, danh sách con người, danh sách các dịch vụ mà tổ chức có sử dụng. Ví dụ: các hợp đồng trên máy tính và trên giấy, danh sách khách hàng, các brochure, danh sách nhân viên cơ quan… Sau khi có danh sách đầy đủ các tài sản, chúng ta có thể hạn chế phạm vi việc triển khai hệ thống ISMS bằng cách loại ra các tài sản mà chúng ta nghĩ rằng chưa cần thiết lập hệ thống bảo vệ (ít ra là trong giai đoạn này). Ví dụ ta chưa xét đến việc bảo vệ hệ thống điện lạnh, hệ thống bàn ghế nội thất hoặc bộ phận bảo dưỡng thiết bị chẳng hạn. Tập hợp tài sản còn lại sẽ là xuất phát điểm của tất cả các bước tiếp theo của hệ thống ISMS.

**Định giá tài sản.** Với danh sách các tài sản cần xem xét bảo vệ, chúng ta phải tiến hành đánh giá giá trị của chúng. Đây là một công tác không khó nếu ta xét giá trị tài sản bằng với chi phí để ta có nó. Tuy nhiên, công tác này trở nên nan giải hơn nhiều nếu chúng ta xét đến (và chúng ta cần phải xét đến) giá trị của tài sản thông qua chi phí mà đối thủ cạnh tranh của chúng ta muốn có nó, thiệt hại nếu chúng ta mất hoặc bị lộ nó. Ví dụ như sơ đồ kết nối mạng chẳng hạn. Chúng ta mất một số ngày với một số chuyên gia để xây dựng sơ đồ nên giá thành để có nó có thể tính được và không lớn. Nhưng nếu chúng ta lộ sơ đồ mạng ra thì ta sẽ có hậu quả gì ? thiệt hại là bao nhiêu tiền ? bị xâm nhập qua đó chúng ta sẽ mất uy tín, mất khách hàng thì kinh doanh sẽ thiệt hại bao nhiêu ? Nếu chúng ta suy luận "dông dài " quá thì bản sơ đồ mạng có khi có giá hơn cả chiếc … Rolls-Royce và phải mua một két sắt để giữ nó với lệnh mở ra chỉ có giám đốc được ký. Còn nếu chúng ta xét đơn giản là một thiết kế với 5 ngày công\*người thì lại quá đơn giản, để đâu cũng được. Cái khó của đánh giá giá trị tài sản là sao cho vừa phải. Đây chính là khó khăn đầu tiên cần vượt qua để xây dựng ISMS. Chuyển giá trị từ định lượng (bao nhiêu tiền) qua định tính (rất đắt/đắt/rẻ…) là một phương án có thể làm đơn giản hóa khâu định giá này. Chuyên gia tư vấn có thể giúp chúng ta có được một đánh giá vừa phải và được chấp nhận ở đa số các tổ chức khác để chúng ta tham chiếu.

**Xác định các hiểm nguy (threat).** Bước tiếp theo là xác định các threat (theo tiếng Anh). Ý tưởng ở đây là phải liệt kê ra các hiểm nguy, đe dọa có thể đối với khối tài sản mà chúng ta đã liệt kê ở trên. Chúng ta cần liệt kê hết, kể cả những đe dọa rất xa vời như ngày tận thế, đến những hiểm nguy cụ thể hơn như mất mật khẩu, mất máy tính xách tay. Vì tính chất liệt kê hết những mối đe dọa mà chưa tính đến liệu nó có thể xảy ra trên thực tế hay chỉ do chúng ta tưởng tượng ra, cho nên tôi chọn cách dịch từ threat là hiểm nguy hay đe dọa.

**Tính toán các nguy cơ (risk).** Như vậy chúng ta đã có 2 thứ trong tay, đó là danh sách tài sản cùng giá trị của chúng và tập hợp các hiểm nguy. Giờ chúng ta sẽ liệt kê dạng “vét cạn” mỗi hiểm nguy với mỗi tài sản. Với mỗi cặp (tài sản, hiểm nguy) chúng ta cần đưa ra đánh giá khả năng nó xảy ra trên thực tế thế nào. Nói theo thuật ngữ khoa học là tính xác suất của hiểm nguy biểu thị dưới dạng liệu nó xảy ra bao nhiêu lần trong tháng, trong năm. Đây là một đánh giá khó khăn và rất kỹ thuật. Ví dụ, chúng ta có 10 nhân viên, mỗi người có 2 mật khẩu. Vậy khả năng lộ mật khẩu là bao nhiêu trong tháng, trong năm? Với tình hình của tổ chức ta, chúng ta có thể bị lộ trung bình 1 mật khẩu trong 1 tháng hay không? Danh sách khách hàng của chúng ta với các thông tin về người quyết định cùng số phone, khả năng tài chính của họ liệu có bị lộ 1 lần trong 1 năm không? Nếu chúng ta làm được những đánh giá này thì thật tuyệt vời vì chúng ta có thể lượng hóa tất cả những nguy cơ do mất an ninh gây ra. Trên thực tế, việc này không đơn giản nên người ta có thể chấp nhận đánh giá dạng định tính, không chính xác nhưng dễ làm hơn. Ví dụ như việc mất mật khẩu xảy ra với nguy cơ “cao”, lộ bảng lương cán bộ công nhân viên xảy ra với khả năng “thấp”.

**Tính toán thiệt hại.** Nếu chúng ta làm tốt các bước trên thì bước đánh giá thiệt hại khi mất an ninh chỉ còn là bài toán giỏi các phép tính số học. Chúng ta có thể lấy tích của giá trị tài sản với khả năng mất chúng để lượng giá được khả năng mất tiền trong một năm nếu chúng ta cứ tiếp tục duy trì hoạt động của tổ chức như hiện nay. Với những nguy cơ lớn và giá trị tài sản mất cao (ví dụ như lộ các thiết kế với công ty chuyên thiết kế thời trang chẳng hạn) thì thiệt hại nhiều khi có thể biểu diễn dạng khả năng công ty phải đóng cửa. Ở phần này, ta không có công thức sẵn sàng để sử dụng, mà chúng ta có thể, và cần phải, đề xuất cách thức tính phù hợp với nhu cầu của tổ chức. Ví dụ một cách tính khác là:

Thiệt hại = xác suất xảy ra sự cố + hậu quả của sự cố + giá trị tài sản bị mất, trong đó các thành phần của công thức đều được định tính hóa cho đơn giản như “hậu quả sự cố” bằng điểm 3/2/1 ứng với mức cao/vừa/thấp.

Với các kết quả tính toán các thiệt hại có thể xảy ra, chúng ta đứng trước câu hỏi: vậy giờ chúng ta cần làm gì?

**Biện pháp giảm thiểu nguy cơ (risk).** Đứng trước nguy cơ cùng lượng giá thiệt hại, chúng ta có thể có mấy lựa chọn:

- Chấp nhận. Không làm gì thêm cả và chấp nhận thiệt hại nếu nguy cơ trở thành hiện thực.

- Giảm thiểu. Cần có các biện pháp để giảm thiểu khả năng xảy ra nguy cơ xuống mức độ có thể chấp nhận được. Đây là lựa chọn phổ biến nhất khi chúng ta bắt tay vào xây dựng ISMS.

- Chuyển tiếp nguy cơ. Tìm cách để chia sẻ nguy cơ này với đối tác khác. Hình thức phổ biến nhất là mua bảo hiểm để tổ chức bảo hiểm sẽ cùng chia sẻ thiệt hại cho ta nếu nguy cơ xảy ra thật.

**Các giải pháp để giảm thiểu nguy cơ.** Nếu chúng ta chọn phương án giảm thiểu thì chúng ta có ngay một câu hỏi tiếp theo là giảm thiểu bằng biện pháp nào. Đây là công đoạn mà các nhà kỹ thuật phải vào cuộc. Để bảo vệ một tài sản thông tin hoặc liên quan tới thông tin, thông thường chúng ta có mấy biện pháp:

- Xây dựng hệ thống bảo vệ bằng các trang thiết bị chuyên dụng như tường lửa, phát hiện xâm nhập, chống xâm nhập, thẻ mật khẩu một lần…

- Tăng thêm nhân viên về số lượng và/hoặc chất lượng.

- Đào tạo huấn luyện nhân viên.

- Xây dựng các qui trình, hướng dẫn, biểu mẫu để mọi người phải tuân thủ.

- Xác định trách nhiệm cá nhân thật rõ ràng. Một thực tế là ai cũng mất trách nhiệm khi phần việc đó không qui định là mình phải chịu trách nhiệm. Vì vậy, qui định rõ ai chịu trách nhiệm tới đâu với từng tài sản, từng nguy cơ nếu xảy ra là một công tác bắt buộc và được nhấn mạnh trong công cuộc xây dựng hệ thống ISMS.

- Xây dựng hệ thống dự phòng để nếu xảy ra cả những nguy cơ lớn nhất thì chúng ta cũng không bị “đóng cửa”.

Để thực hiện khâu này, nhà tư vấn tốt nhất, theo tôi là ISO27002. Đây chính là tập hợp các best practices, tạm dịch là ứng xử tốt nhất, để giảm thiểu các nguy cơ về an ninh thông tin. Đây là tập hợp các giải pháp, các lời khuyên đã được đúc kết, trải nghiệm ở nhiều nơi trên thực tế để nâng cao mức độ an ninh an toàn của một hệ thống CNTT. Vì vậy, chúng ta có thể tham khảo, xem xét lựa chọn các giải pháp từ ISO27002 để áp dụng cho tổ chức của mình.

**Đánh giá chi phí cho giải pháp và đưa ra quyết định.** Đề ra các biện pháp giảm thiểu nguy cơ,như đã nói ở trên là, một công việc rất kỹ thuật. Vì vậy, chi phí để thực hiện nó là điều mà các nhà kỹ thuật rất ít quan tâm, hoặc không có khả năng đánh giá. Chúng ta đừng quên là các biện pháp trên là để bảo vệ tài sản. Và tài sản có giá trị nhất định (thường là hữu hạn) của nó.

Chúng ta không thể đầu tư 10 đồng để bảo vệ tài sản trị giá 5 đồng. Nếu các bạn trả lời “có thể” thì tôi nghĩ chúng ta nên quay lại phần định giá giá trị tài sản. Có lẽ nó còn quan trọng hơn điều chúng ta nghĩ hoặc chúng ta còn đánh giá thiếu điều gì chăng? Ở bước này, chúng ta sẽ phải làm một bài toán kinh tế thuần túy là đầu tư bao nhiêu để giảm thiểu thiệt hại xuống bao nhiêu. Trả lời câu hỏi “kế họach này có đúng trên phương diện kinh tế không? Sau khi đã giảm thiểu nguy cơ và giá trị có thể bị mất, nguy cơ và thiệt hại còn lại có chấp nhận được hay không đối với tổ chức?”. Với mỗi câu trả lời “không”, chúng ta lại phải rà soát lại tất cả những công đoạn đã thực hiện ở trên, xem xét lại các phương án, giải pháp để giảm thiểu nguy cơ cùng chi phí của nó. Cho đến khi tất cả các câu trả lời là “có” thì chúng ta đã hòan thành một kế họach xây dựng hệ thống ISMS.

**Triển khai ISMS.** Sau khi bản kế hoạch xây dựng hệ thống ISMS bao gồm danh sách tài sản cùng giá trị của nó, các nguy cơ cùng thiệt hại có thể, các phương án, biện pháp để giảm thiểu nguy cơ và thiệt hại xuống mức chấp nhận được đối với tổ chức, thì công tác tiếp theo là đưa bản kế họach ra thực tế. Các hoạt động cụ thể của công tác triển khai này là:

- Thiết kế lại, đầu tư bổ sung các thành phần kỹ thuật.

- Xây dựng các qui định, qui trình, hướng dẫn và, đặc biệt là triển khai đào tạo, hướng dẫn thực hiện để những qui định này được nắm bắt bởi mọi nhân viên, cán bộ của tổ chức. Đây là một phần việc rất lớn vì chúng ta phải thay đổi thói quen trong suy nghĩ, trong hành động của mọi người. Đồng thời, tất cả các thành viên, đặc biệt những người lãnh đạo tổ chức phải hiểu rõ và thực hiện nghiêm túc các qui định của cơ quan. Đây chính là yếu tố quyết định. Quyết định đến mức nếu lãnh đạo không quan tâm đủ, không dành đủ thời gian cho xây dựng ISMS thì giải pháp tốt nhất là đừng làm ISMS cho đến khi suy nghĩ của lãnh đạo thay đổi.

Nếu chúng ta đi đến đây, tôi nghĩ là chúng ta đã có được hệ thống ISMS. Hệ thống này tốt hay xấu, hòan thiện hay không, chúng ta khó mà khẳng định, cũng như khó mà làm cho người ngoài, đối tác, khách hàng của chúng ta tin tưởng vào hệ thống ISMS này. Đây là lúc các tổ chức đánh giá chứng chỉ (Certification Body) vào cuộc. Họ sẽ kiểm tra hệ thống ISMS của chúng ta và cấp một chứng nhận là hệ thống này “đạt chuẩn” nếu nó thỏa mãn các yêu cầu của chứng chỉ. Vậy thì tổ chức đánh giá họ sẽ làm thế nào?

**Đánh giá và cấp chứng chỉ ISO27001.** Nhìn chung, quá trình đánh giá để cấp chứng chỉ sẽ được thực hiện bởi một tổ chức có thẩm quyền. Tổ chức này không thể là tổ chức đã tư vấn về ISMS cho chúng ta để tránh trường hợp “vừa đá bóng, vừa thổi còi”. Qui trình đánh giá thường gồm 2 giai đoạn cơ bản là:

- Đánh giá trên tài liệu để đảm bảo tính đầy đủ của hệ thống văn bản giấy tờ. Nói một cách khác là kiểm tra “đã viết hết nhưng gì định làm” chưa?

- Đánh giá trên thực tế để đảm bảo những điều chúng ta định làm là được thực hiện trên thực tế. Nói một cách khác là kiểm tra “làm đúng những gì đã viết” chưa?

Tôi không đi sâu vào quá trình kiểm tra này (vì không biết rõ), nên chỉ đề cập tới một ý trong phương pháp mà tổ chức kiểm tra để cấp chứng chỉ thực hiện. Với quá trình kiểm tra, Statement of Applicability (SoA), hay điều khoản thực hiện, đóng một vai trò quan trọng. Trong ISO27001, các SoA được phát biểu dưới dạng các “Control objectives and controls” và hiện nay ISO27001 có 133 SoA.

Hãy xem xét quá trình học và thi thông thường. Để kiểm tra kiến thức chúng ta xem chúng ta nắm bắt được bao nhiêu trong quá trình học, thầy giáo thường không bắt chúng ta kể lại kiến thức đã học miêu tả trong tài liệu, mà bắt chúng ta phải trả lời các câu hỏi. Các câu hỏi là một cách tốt nhất để kiểm tra dưới một góc độ khác kiến thức chúng ta học được.

Việc kiểm tra để cấp chứng chỉ (tức là xác nhận hệ thống đạt chuẩn) tốt nhất được thực hiện qua các điều khỏan SoA. Ví dụ của một SoA là “Ownership of assets” có yêu cầu là “All information and assets associated with information processing facilities shall be owned by a designated part of the organization”. Tạm dịch là yêu cầu phải có tính sở hữu đối với tài sản. Cụ thể là tất cả các tài sản đều phải có người/tổ chức sở hữu. Nói khác nữa là không được có tài sản mà không biết ai là người sở hữu, chịu trách nhiệm về nó. Với điều khỏan kiểm tra này, có thể nói là người đánh giá rất dễ dàng xác định chúng ta có thỏa mãn yêu cầu hay không. Với bộ 133 điều khỏan kiểm tra người đánh giá có thể yên tâm rằng tất cả các vấn đề liên quan tới bảo đảm an ninh thông tin đều được rà soát. Người đánh giá không bị “cuốn” theo logic của người xây dựng hệ thống ISMS thông qua lộ trình xuất phát từ tài sản. Nếu hoạt động của chúng ta không liên quan tới một điều khoản kiểm tra (control) nào đó, chúng ta có thể bỏ nó ra khỏi phạm vi đánh giá với điều kiện phải giải thích rõ tại sao chúng ta loại bỏ.

**Lời kết.** Xây dựng hệ thống ISMS để lấy chứng chỉ ISO27001 đảm bảo cho thông tin được an ninh, an toàn và bảo mật đang được nhiều doanh nghiệp Việt nam quan tâm. Đây là một tín hiệu tốt, một thước đo trình độ phát triển của ứng dụng CNTT trong đời sống kinh tế - xã hội Việt nam. Hy vọng rằng những trình bày trên của tôi có thể giúp các bạn có một cách tiếp cận, một cách suy nghĩ để hiểu rõ hơn những vấn đề quan trọng, nhưng còn khá mới mẻ với chúng ta – ISMS và ISO27001.

**TS. Trịnh Ngọc Minh**hiện là giảng viên của Viện Công Nghệ Kỹ Thuật Sài Gòn – SaigonCTT. Mọi thông tin trao đổi về bài viết, vui lòng liên hệ info@saigonctt.com.vn