ĐẠI HỌC QUỐC GIA HÀ NỘI

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

TRẦN KIÊN

TÓM TẮT LUẬN VĂN

XÂY DỰNG QUY TRÌNH BẢO ĐẢM AN TOÀN THÔNG TIN THEO CHUẨN ISO27001 CHO CÁC DOANH NGHIỆP VỪA VÀ NHỎ TẠI VIỆT NAM

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

Sự phát triển của Internet Việt Nam đã đạt được nhiều thành quả to lớn trong 15 năm qua, với số lượng gần 4,8 triệu thuê bao truy nhập Internet băng rộng cố định, hơn 3,2 triệu hộ gia đình có kết nối Internet, 100% các Bộ ngành, tỉnh thành phố có cổng thông tin điện tử. Hiện tại, theo xu hướng ứng dụng công nghệ thông tin vào cuộc sống ngày càng sâu rộng thì các loại hình tội phạm mạng cũng như các nguy cơ làm mất an toàn thông tin ngày càng đa dạng và khó phòng chống hơn. Hệ thống máy tính của các tổ chức thường xuyên phải đối phó với các cuộc tấn công, xâm nhập trái phép, gây rò rỉ, mất mát thông tin, thậm chí dừng hoạt động, ảnh hưởng tiêu cực đến tiến độ, chất lượng công việc, kéo theo đó là các tổn thất về kinh tế, uy tín của tổ chức và thậm chí là ảnh hưởng tới an ninh quốc gia.

Các sự cố liên quan đến an toàn thông tin (ATTT) tại Việt Nam

Theo báo cáo của nhiều tổ chức quốc tế về an toàn thông tin, Việt Nam là một trong các mục tiêu hàng đầu trong khu vực của các tấn công gián điệp có tổ chức, mà mục tiêu của các cuộc tấn công này là các cơ quan, tổ chức

quan trọng thuộc chính phủ và các tổ chức có sở hữu các hạ tầng thông tin trọng yếu.

Theo ghi nhận của trung tâm VNCERT số lượng các loại vụ việc, sự cố mất an toàn thông tin trong những năm qua được phát hiện và xửa lý ngày càng tăng. Trong 3 năm 2013-2015 trung tâm VNCERT ghi nhận 4.954.853 lượt địa chỉ IP của Việt Nam bị các mạng máy tính ma chiếm quyền điều khiển để đánh cắp thông tin hoặc phát tán mã độc, phát tán thư điện tử rác và tấn công mạng, trong đó có tới 12.480 lượt địa chỉ IP tĩnh của các cơ quan nhà nước nằm trong các mạng này. Chỉ tính riêng 6 tháng đầu năm 2016 các sự cố này đã trên 127.000. Trong đó, Phishing: 8.758; Deface: 77.160; Malware: 41.712.[1] Tâm điểm về các sự cố mất an toàn thông tin năm 2016 là vụ tin tặc tấn công vào vào một số màn hình hiển thị thông tin chuyến bay tại khu vực làm thủ tục bay của các sân bay như: Sân bay Tân Sơn Nhất, Sân bay Nội Bài, Sân bay Đà Nẵng, Sân bay Phú Quốc vào chiều 29 tháng 07 năm 2016. Các màn hình của sân bay đã bị chèn những hình ảnh và nội dung câu chữ xúc phạm Việt Nam và Philippines, xuyên tạc các nội dung về biển Đông. Hệ

[1] Nguồn: Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam

thống phát thanh của sân bay cũng phát đi những thông điệp tương tự. Đồng thời website của Việt Nam Airlines cũng bị hack với 411.000 dữ liệu của hành khách đi máy bay đã bị hacker thu thập và phát tán. Vụ việc đã gây thiệt hại làm cho hơn 100 chuyến bay bị ảnh hưởng, trong đó hàng chục chuyến bay bị chậm giờ từ 15 phút cho đến hơn 1 tiếng. Tại sân bay Nội Bài tất cả các màn hình và loa phát thanh tạm thời ngưng hoạt động để ngăn chặn hacker phát thông tin giả mạo. Các hãng hàng không phải sử dụng loa tay để thông báo cho khách.

Bên cạnh những rủi ro về an toàn thông tin (ATTT) do bị tấn công phá hoại có chủ đích, đáng chú ý là nhiều đơn vị không biết những sự cố liên quan đến an toàn thông tin đang nằm trong hệ thống mạng của mình. Các nguyên nhân chủ yếu là: Các quy trình quản lý, vận hành không đảm bảo; việc quản lý quyền truy cập chưa được kiểm tra và xem xét định kỳ; nhận thức của nhân viên trong việc sử dụng và trao đổi thông tin chưa đầy đủ; năng lực của các cán bộ kỹ thuật còn yếu, thiếu cán bộ chuyên môn và thiếu trang bị kỹ thuật tối thiểu… Do đó, ngoài các biện pháp kỹ thuật, tổ chức cần xây dựng và áp dụng các chính sách, quy định, quy trình vận hành phù hợp để giảm thiểu rủi ro.

Giải pháp ISO27001

Giải pháp toàn diện và hiệu quả nhất để giải quyết vấn đề trên là hệ thống của doanh nghiệp cần xây dựng, triển khai quy trình bảo vệ ATTT theo tiêu chuẩn ISO27001. Việc triển khai quy trình đáp ứng tiêu chuẩn ISO27001 sẽ giúp hoạt động đảm bảo ATTT của tổ chức được quản lý chặt chẽ, đạt được một số lợi ích sau:

- Bảo vệ thông tin của tổ chức, khách hàng và đối tác.

- Nhân viên tuân thủ và có thói quen đảm bảo ANTT.

- Hoạt động đảm bảo ANTT luôn được duy trì và cải tiến.

- Hoạt động nghiệp vụ trọng yếu của tổ chức không bị gián đoạn.

- Nâng cao uy tín của tổ chức, tăng sức mạnh cạnh tranh.

Thực trạng triển khai ISO27001 tại Việt Nam

Hiện tại tại Việt Nam việc xây dựng, triển khai quy trình bảo vệ ATTT theo tiêu chuẩn ISO27001 còn rất hạn chế. Chủ yếu là các doanh nghiệp lớn hoặc doanh nghiệp có vốn đầu tư nước ngoài mới quan tâm đến việc đầu tư, xây dựng và triển khai.

- Tháng 2/2006: Tổng cục Tiêu chuẩn Đo lường Chất lượng Việt Nam đã ban hành tiêu chuẩn TCVN 7562: 2005 – Công nghệ thông tin – Mã thực hành quản lý an toàn thông tin, (tương đương với tiêu chuẩn ISO/IEC 17799: 2000). Tiêu chuẩn này đề ra các hướng dẫn thực hiện hệ thống quản lý an ninh thông tin làm cơ sở cho ISO27001.

- Tháng 1/2007: Công ty CSC Việt Nam (Computer Sciences Corporation) đã trở thành đơn vị đầu tiên có được chứng nhận ISO27001.

- Đến tháng 7/2013 ở Việt Nam có 5 đơn vị (CSC Việt Nam, FPT IS, FPT Soft, GHP FarEast, ISB Corporation Vietnam…) đã đạt chứng nhận ISO27001 và hơn 10 đơn vị (HPT Soft, VietUnion, Quantic…) đang trong quá trình triển khai ứng dụng tiêu chuẩn này.

- Đến hết năm 2012, Việt Nam đã có 249 chứng chỉ ISO27001.

- Năm 2014, Việt Nam được cấp 94 chứng chỉ ISO27001, nhiều hơn so với năm 2013 và 2012 lần lượt là 55 và 50 chứng chỉ.

Cũng qua số liệu này, chúng ta có thể thấy số đơn vị đạt chứng nhận ISO27001 tại Việt Nam khá khiêm tốn so với Nhật Bản (53290 chứng nhận), Trung Quốc (8294 chứng nhận), Malaixia (759 chứng nhận). Một trong những nguyên nhân của tình trạng này là chi phí để đạt chứng nhận ISO27001 khá cao, bao gồm các chi phí về tư vấn, cấp chứng nhận và đặc biệt là chi phí doanh nghiệp phải bỏ ra để thực hiện các biện pháp kiểm soát rủi ro.

Vấn đề của các doanh nghiệp vừa và nhỏ tại Việt Nam trong việc áp dụng và triển khai ISO27001

Các doanh nghiệp ở Việt Nam chủ yếu là các doanh nghiệp có quy mô vừa và nhỏ[2], chiếm 94.8%[3] nên nguồn lực còn hạn chế nên sự quan tâm đến lĩnh vực áp các chuẩn quản lý chất lượng quốc tế như ISO27001 còn chưa nhiều. Nguyên nhân của thực trạng này là như sau:

[2] Ở Việt Nam, theo Điều 3, Nghị định số 56/2009/NĐ-CP ngày 30/6/2009 của Chính phủ, quy định số lượng lao động trung bình hàng năm từ 10 người trở xuống được coi là doanh nghiệp siêu nhỏ, từ 10 đến dưới 200 người lao động được coi là Doanh nghiệp nhỏ và từ 200 đến 300 người lao động thì được coi là Doanh nghiệp vừa.

[3] Nguồn: "Báo cáo tổng quan về tình hình doanh nghiệp" trong báo cáo phục vụ Hội nghị Thủ tướng Chính phủ với doanh nghiệp

- Nhận thức của toàn tổ chức về việc đảm bảo ANTT, lợi ích triển khai áp dụng Hệ thống quản lý ANTT chưa cao.

- Chi phí để áp dụng khá cao, trong đó đặc biệt là chi phí doanh nghiệp phải bỏ ra để thực hiện các biện pháp kiểm soát rủi ro.

- Khó khăn trong triển khai: phối hợp không tốt giữa các bộ phận, không cam kết nguồn lực tham gia và áp lực về thời gian.

- Sự quan tâm, cam kết thực hiện của lãnh đạo chưa cao.

- Đầu tư (nguồn lực, tài chính) còn bị hạn chế.

Mục tiêu của luận văn

Với mong muốn đóng góp một phần nhỏ công sức cho nền doanh nghiệp nước nhà trong việc đảm bảo an toàn thông tin, nơi mà tỷ lệ doanh nghiệp vừa và nhỏ chiếm đa số, luận văn sẽ tập trung tìm hiểu ISO27001, chọn ra một doanh nghiệp vừa và nhỏ đặc trưng và tiến hành xây dựng quy trình đáp ứng tiêu chuẩn ISO27001 cho doanh nghiệp này với những công sức về mặt chi phí và thời gian đã được giảm thiểu, phù hợp với đặc trưng của các doanh nghiệp vừa và nhỏ khi chỉ có nguồn lực (chi phí và thời

gian) hạn chế. Với tinh thần đó, luận văn được bố cục thành 04 chương chính như sau:

- Mở đầu

Phần này sẽ nêu ra các vấn đề, thực trạng trong việc áp dụng các tiêu chuẩn đảm bảo an toàn thông tin theo chuẩn ISO27001 trong các doanh nghiệp tại Việt Nam, vấn đề gặp phải của các doanh nghiệp vừa và nhỏ khi tiến hành áp dụng tiêu chuẩn này và đưa ra mục tiêu trong việc giải quyết vấn đề của luận văn.

- Chương 1: Giới thiệu ISO27001

Chương này sẽ tập trung giới thiệu khái niệm ISO27001, cấu trúc, nội dung, các điều khoản phải tuân thủ khi áp dụng ISO27001.

- Chương 2: Khảo sát doanh nghiệp SME cụ thể về bảo đảm an toàn thông tin

Chương này sẽ chọn ra một doanh nghiệp SME tiêu biểu trong việc đảm bảo an toàn thông tin, giới thiệu về cơ cấu tổ chức, nhân sự, lĩnh vực hoạt động kinh doanh… cũng như yêu cầu đảm bảo an toàn thông tin của các bên liên quan. Sau đó sẽ tiến hành khảo sát về thực trạng bảo đảm

an toàn thông tin của doanh nghiệp SME đã lựa chọn dựa trên việc liệt kê các tài sản của doanh nghiệp, phân tích các rủi ro, các nguy cơ và đưa ra các biện pháp kiểm soát.

- Chương 3: Đề xuất bộ quy trình cho doanh nghiệp SME đã lựa chọn

Sau khi tiến hành khảo sát doanh nghiệp SME đã lựa chọn ở chương 2, chương này sẽ đề xuất xây dựng quy trình, chính sách, biện pháp, thủ tục… để đảm bảo an toàn thông tin, giải quyết các vấn đề liên quan đến an toàn thông tin mà doanh nghiệp trên gặp phải theo chuẩn ISO27001.

- Chương 4: Kết luận

Sau khi đề xuất, xây dựng bộ quy trình ở chương 3, chương này sẽ đánh giá những mặt được và mặt chưa được của bộ quy trình đã xây dựng được. Sau đó sẽ tiến hành đề xuất những hướng phát triển tiếp theo của luận văn, đó là tiếp tục tìm hiểu các doanh nghiệp vừa và nhỏ đặc trưng khác trong việc bảo đảm an toàn thông tin, rút ra những nét đặc trưng để xây dựng một nền tảng quy trình chung, với mục đích đóng góp một phần công sức cho các doanh nghiệp vừa và nhỏ tại Việt Nam trong việc đảm bảo an toàn thông tin, một vấn đề khá nhức nhối hiện nay.

Các kết quả luận văn đã làm được

Với dân số 90 triệu người, trong đó gần 44% sử dụng Internet, nhiều người truy cập sử dụng Internet trên thiết bị di động, thị trường công nghệ đang rất phát triển tại Việt Nam. Việt Nam trở thành mục tiêu của các nhà phát triển ứng dụng và được các nhà đầu tư trong và ngoài nước để mắt. Nhiều tập đoàn đa quốc gia như Samsung và Intel đang có sự hiện diện vô cùng lớn tại đây, trong khi các startup công nghệ của Việt Nam cũng nhanh chóng nhập cuộc. Tuy chưa có số liệu chính thức nào về bức tranh khởi nghiệp Việt Nam, tập đoàn Softbank của Nhật Bản ước tính có khoảng 1.500 startup đang hoạt động, trong đó phần lớn là các startup liên quan đến công nghệ, từ con số có thể thấy Việt Nam có tỉ lệ startup trên số dân cao hơn hẳn các láng giềng như Trung Quốc, Indonesia và Ấn Độ.[4]

Đặc điểm của các startup công nghệ ở Việt Nam là quy mô mới chỉ ở mức vừa và nhỏ, các doanh nghiệp này tập trung phần lớn công sức, thời gian vào việc phát triển kinh doanh, tìm kiếm những ý tưởng, sáng tạo, sản xuất sản phẩm ứng dụng công nghệ mới… nhưng chưa để ý, dành thời gian, công sức, chưa hiểu rõ các phương pháp tiếp

[4] Theo http://ictnews.vn

cận đến việc đảm bảo an toàn thông tin cho doanh nghiệp của mình.

Sau khi lựa chọn một doanh nghiệp vừa và nhỏ đặc thù, với lĩnh vực hoạt động liên quan đến công nghệ thông tin, cụ thể là sản xuất và phân phối game online trên điện thoại di động, một ngành mới nổi và rất nhiều tiềm năng phát triển tại Việt Nam, tiến hành khảo sát về thực trạng đảm bảo an toàn thông tin đối với doanh nghiệp này, xác định các rủi ro, nguy cơ và đưa ra các biện pháp kiểm soát, luận văn đã xây dựng được cho doanh nghiệp này những chính sách, quy trình, quy định trong việc đảm bảo an toàn thông tin theo đúng tiêu chuẩn ISO27001, cụ thể như sau:

1. 01 chính sách về các lĩnh vực:

- Kiểm soát truy cập

- Quản lý truyền thông và hoạt động

- An ninh môi trường và vật lý

- An ninh cá nhân

- Đào tạo nhân viên

2. 04 quy trình:

- Quy trình đo lường của hệ thống quản lý an toàn thông tin

- Quy trình về quản lý source code, các bản mềm tài liệu

- Quy trình về giáo dục nhận thức, đào tạo về an toàn thông tin

- Quy trình hành động phòng ngừa đối với hệ thống quản lý an toàn thông tin

3. 02 quy định:

- 01 quy định chung đối với nhân viên

- 01 quy định những việc phải làm và những việc không được làm đối với nhân viên mới.

Các tiêu chuẩn của ISO27001 đã được áp dụng

01 chính sách, 04 quy trình và 02 quy định đã tuân thủ các tiêu chuẩn sau của ISO27001:

- 7 điều khoản bắt buộc về phạm vi tổ chức, lãnh đạo, lập kế hoạch, hỗ trợ, vận hành hệ thống, đánh giá hiệu năng hệ thống, cải tiến hệ thống.

- Các lĩnh vực kiểm soát liên quan bao gồm: chính sách ATTT, ATTT trong tổ chức, ATTT nhân sự, quản lý tài sản, kiểm soát truy cập, ATTT vật lý và nơi làm việc, ATTT trong quá trình vận hành, quản lý sự cố ATTT, đảm bảo tính hoạt động liên tục trong trường hợp thảm họa và sự tuân thủ.

Những lợi điểm mà những chính sách, quy trình và quy định mang lại

Luận văn đã giải quyết được những khó khăn mà một doanh nghiệp vừa và nhỏ đã gặp phải trong việc đảm bảo an toàn thông tin:

- Nâng cao nhận thức của toàn tổ chức về việc đảm bảo ANTT

- Tiết kiệm chi phí doanh nghiệp phải bỏ ra để thực hiện các biện pháp kiểm soát rủi ro, mọi chi phí về nguồn lực và tài chính được giảm thiểu phù hợp với đặc trưng của một doanh nghiệp vừa và nhỏ như: về mặt nhân sự tham gia được giảm thiểu bao gồm 01 nhân viên phụ trách chính trong việc xây dựng và đảm bảo quy trình an toàn thông tin theo tiêu chuẩn ISO27001 trong tổ chức, các lãnh đạo và toàn thể nhân viên phòng ban, về mặt thời

gian xây dựng và triển khai các chính sách, quy trình và quy định ngắn, dễ áp dụng cho các doanh nghiệp vừa và nhỏ, áp dụng nhiều công nghệ tiên tiến trong việc triển khai như các công cụ phần mềm trong việc quản lý các tài liệu, source code, các công cụ quản lý các sự cố, công việc của nhân viên và cuối cùng, sẽ dẫn đến tiết kiệm chi phí tài chính phải bỏ ra cho doanh nghiệp.

- Việc triển khai các chính sách, quy trình và quy định trong việc đảm bảo an toàn thông tin được tinh giản và nâng cao hiệu quả trong việc phối hợp, trao đổi giữa các bộ phận.

- Nâng cao nhận thức đối với các cam kết thực hiện của lãnh đạo.

Tuy nhiên với thời gian khảo sát ngắn có thể chưa liệt kê được tất cả các vấn đề mà doanh nghiệp gặp phải trong việc đảm bảo an toàn thông tin, khi tiến hành các chính sách, quy trình và quy định, sẽ gặp phải những vấn đề phát sinh, cần tiếp tục điều chỉnh, sửa đổi và bổ sung sao cho phù hợp nhất với thực tế của doanh nghiệp.

Hướng phát triển tiếp theo

Hướng tiếp theo, tôi có đề xuất sẽ tiếp tục tiến hành khảo sát các doanh nghiệp vừa và nhỏ đặc trưng trong các lĩnh vực khác như công nghiệp, dịch vụ về vấn đề đảm bảo an toàn thông tin, và xây dựng, triển khai các chính sách, quy trình và quy định cho các doanh nghiệp này. Từ những kết quả thực tiễn thu được, luận văn mong muốn từ đó khái quát ra một bộ khung chính sách, quy trình và quy định đảm bảo về an toàn thông tin theo chuẩn ISO27001 cho các doanh nghiệp vừa và nhỏ tại Việt Nam.

Hy vọng với bộ khung chính sách, quy trình và quy định cho các doanh nghiệp vừa và nhỏ tại Việt Nam trong việc đảm bảo an toàn thông tin theo chuẩn ISO27001 này, sẽ giúp đỡ được một phần nào cho các doanh nghiệp vừa và nhỏ tại Việt Nam, hiện đang chiếm gần 95% tổng số các doanh nghiệp, đảm bảo an toàn về an toàn thông tin cho các công ty startup, góp một phần nhỏ bé vào công cuộc xây dựng và bảo vệ đất nước.