NÂNG CAO NHẬN THỨC VỀ RỦI RO AN NINH MẠNG TRONG LĨNH VỰC KẾ TOÁN

RAISING AWARENESS OF CYBERSECURITY RISKS IN ACCOUNTING

TS. Lương Đức Thuận - TS. Phan Thị Bảo Quyên

Trường Đại học Kinh tế Thành phố Hồ Chí Minh

Tóm tắt

Ngày nay với mức độ kết nối toàn cầu rất lớn và sự phổ biến rộng rãi của mạng xã hội cùng các thiết bị di động, do đó rủi ro bị tấn công mạng và những lỗ hổng dữ liệu đang ngày càng gia tăng. Rủi ro mạng máy tính được xem là một trong các thách thức nghiêm trọng nhất về kinh tế và an ninh thông tin đối với các doanh nghiệp. Từ đó, mục tiêu chính của bài viết là nhằm làm rõ một số vấn đề về rủi ro an ninh mạng và quản lý rủi ro, qua đó hướng đến đề xuất một số giải pháp để giúp nhân viên có thể nâng cao văn hóa nhận thức an ninh mạng trong lĩnh vực kế toán cùng với việc hỗ trợ doanh nghiệp áp dụng các kiến thức quản trị an ninh mạng trong công tác quản lý và điều hành hiện nay.

Từ khóa: An ninh mạng, Chương trình SETA, Kế toán, Quản lý rủi ro, Sự nhận thức rủi ro

Abstract

Today, with a huge level of global connectivity and the widespread availability of social network and mobile devices, the risk of cyberattacks and data breaches is increasing. Computer network risk is considered one of the most serious economic and information security challenges for businesses. From there, the main goal of the article is to clarify some issues about cybersecurity risks and risk management, thereby aiming to propose some solutions to help employees improve the culture of cybersecurity awareness in the field of accounting along with supporting businesses to apply cybersecurity management knowledge in current management and administration.

Keywords: Cybersecurity, SETA program, Accounting, Risk Management, Risk awareness

JEL Classifications: M40, M49, M15

DOI: https://doi.org/10.59006/vnfa-jaa.07202308

1. Giới thiệu

Công nghệ thông tin và truyền thông đã định hình lại việc tạo ra giá trị kinh tế bằng cách cho phép các doanh nghiệp giảm sự phụ thuộc vào tài sản và vốn hữu hình, đề cao vai trò của vốn trí tuệ. Điều này đã khiến hầu hết các thị trường dựa vào các nền tảng internet do con người tạo ra (Starr & cộng sự, 2010). Lợi ích của việc khai thác miền trên mạng là khả năng phát triển mới của các doanh nghiệp khắc phục các ràng buộc về thời gian và địa lý như một yếu tố thúc đẩy các mô hình kinh doanh mới. Tuy nhiên, một tác dụng tiêu cực của sự phụ thuộc vào tên miền này nằm ở phạm vi lỗ hổng bảo mật mà nó gây ra. Các mối đe dọa trên mạng có thể phá vỡ sự an ninh, sự ổn định và bền vững của các tổ chức bằng cách ảnh hưởng đến tính bảo mật, tính toàn vẹn và tính khả dụng của thông tin.

Tác giả Brands & Elam (2021) cho rằng, dữ liệu của tổ chức là tài sản vô giá. Nếu không bảo vệ nó sẽ gây nguy hiểm cho vị thế cạnh tranh, danh tiếng và tính bền vững trong hoạt động. Như Richard Clarke, cựu Điều phối viên Quốc gia về An ninh, bảo vệ Cơ sở hạ tầng và Chống Khủng bố của Hoa Kỳ, đã nói: "***Nếu bạn chi tiêu nhiều hơn cho cà phê hơn là cho bảo mật công nghệ thông tin, bạn sẽ bị tấn công. Hơn nữa, bạn xứng đáng bị tấn công***". Hành động ngay hôm nay để bảo vệ tổ chức của bạn khỏi nguy cơ an ninh mạng.

Như chúng ta đã biết, an ninh mạng là thuật ngữ chuyên dụng trong lĩnh vực công nghệ thông tin. Đây là hệ thống tổng hợp các hoạt động nhằm đảm bảo sự an toàn về thông tin dữ liệu trên máy tính, máy chủ, thiết bị di động khỏi các cuộc tấn công qua Internet. Hiện nay, an ninh mạng luôn là vấn đề được quan tâm đối với nhiều doanh nghiệp và tổ chức. Vì thế, họ không ngừng phát triển và thay đổi hệ thống bảo mật nhằm ngăn chặn và hạn chế tối đa các rủi ro xâm nhập hệ thống mạng trái phép. Trong bài viết này, tác giả tập trung trình bày một số nội dung liên quan vấn đề quản lý rủi ro và hướng đến nâng cao văn hóa nhận thức an ninh mạng của nhân viên

2. Định nghĩa an ninh mạng

Theo khoản 1, Điều 2, Luật An ninh mạng 2018 định nghĩa an ninh mạng là: "*An ninh mạng là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân".*

An ninh mạng thường được sử dụng như một thuật ngữ tương tự cho bảo mật thông tin. Tuy nhiên, an ninh mạng không nhất thiết chỉ là bảo vệ bản thân không gian mạng mà còn bảo vệ những người hoạt động trong không gian mạng và bất kỳ tài sản nào của họ có thể được tiếp cận thông qua không gian mạng (von Solms & van Niekerk, 2013). An ninh mạng bao gồm các công nghệ, quy trình và kiểm soát được thiết kế để bảo vệ hệ thống, mạng và dữ liệu khỏi các cuộc tấn công mạng.

An ninh mạng hiệu quả làm giảm nguy cơ bị tấn công mạng và bảo vệ xã hội, tổ chức và cá nhân khỏi việc khai thác trái phép các hệ thống, mạng và công nghệ. An ninh mạng là một khái niệm bao gồm bảo mật thông tin và đảm bảo thông tin (No & Vasarhelyi, 2017). Do đó, an ninh mạng liên quan đến việc bảo vệ thông tin được đánh giá và truyền qua bất kỳ mạng máy tính nào (Gordon & Loeb, 2006).

Khi số lượng sự cố an ninh mạng tiếp tục gia tăng và các bên liên quan ngày càng lo ngại, các công ty đang dành nguồn lực đáng kể cho các nỗ lực quản lý rủi ro an ninh mạng và các tiết lộ liên quan đến an ninh mạng. Bài báo này mô tả cách kế toán có vị trí duy nhất để hỗ trợ các công ty trong những nỗ lực này trong năng lực tư vấn và đảm bảo. Chúng tôi trình bày một mô hình quản lý rủi ro an ninh mạng hiệu quả và thảo luận về cách năng lực cốt lõi của kế toán viên có thể tăng thêm giá trị đáng kể trong từng giai đoạn trong số năm giai đoạn của mô hình. Ngoài ra, chúng tôi sử dụng một số sự cố an ninh mạng nổi tiếng gần đây làm ví dụ minh họa trong mỗi giai đoạn trong số năm giai đoạn. Chúng tôi kết luận bằng cách thảo luận về các tác động đối với kế toán.

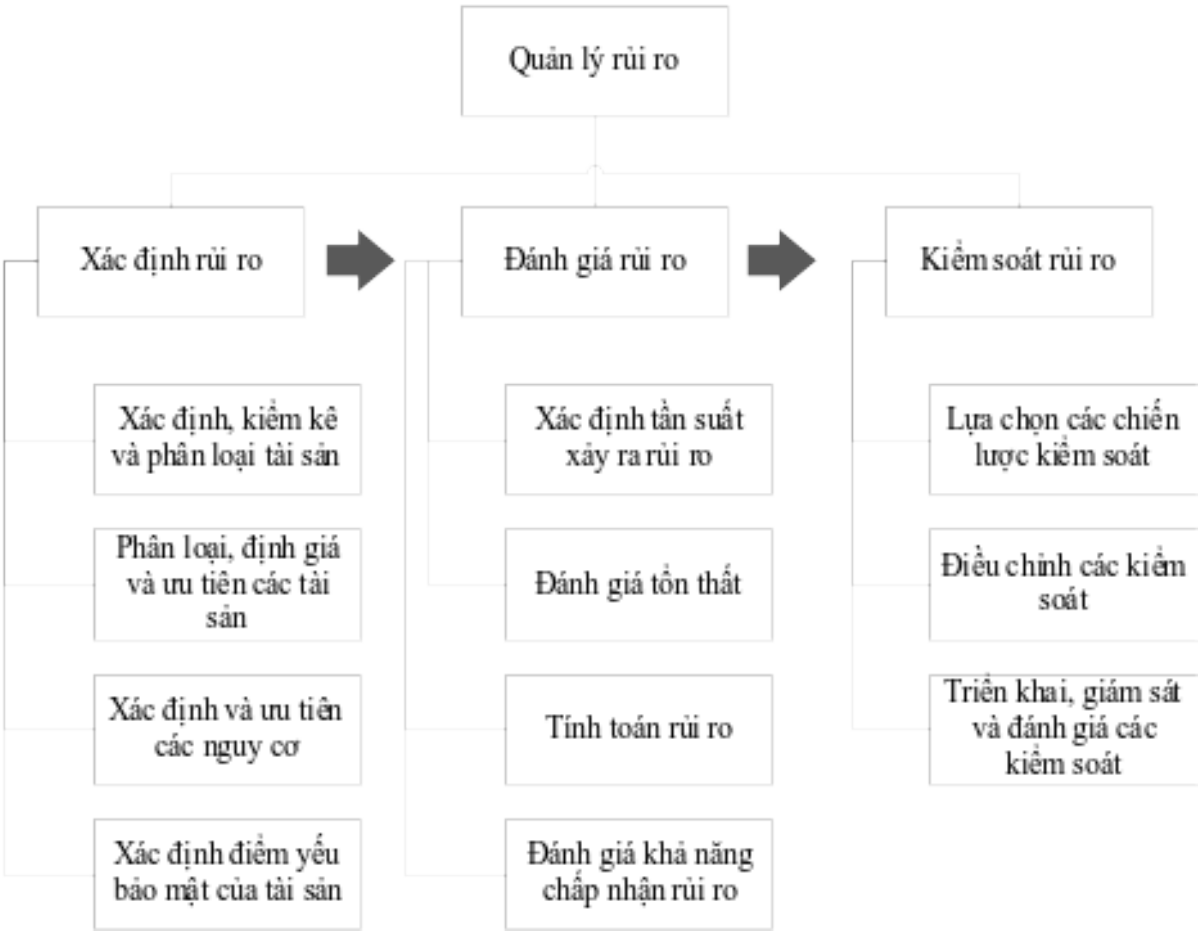
3. Quản lý rủi ro an ninh mạng

Việc xác định và ưu tiên rủi ro là điều cần thiết để quản lý rủi ro hiệu quả. Nếu một công ty không xác định được các rủi ro nhất định hoặc ưu tiên các rủi ro sai, việc quản lý rủi ro chắc chắn sẽ thất bại và dẫn đến những hậu quả bất lợi đáng kể. Điều này đặc biệt đúng trong lĩnh vực an ninh mạng, nơi có vô số các mối đe dọa an ninh mạng luôn thay đổi do tin tặc nghĩ ra.

Theo Sallos & cộng sự (2019), an ninh mạng vẫn là một nhiệm vụ thứ yếu trong hầu hết các mô hình kinh doanh, vì nó cung cấp các cơ hội hạn chế để kiếm tiền và tạo ra giá trị - đó là vấn đề tổ chức. Kiến thức như một cấu trúc xuyên suốt an ninh mạng và mô tả rủi ro tổ chức rộng hơn theo một số cách. Mối liên hệ giữa rủi ro và kiến thức đã được Max-Neef (2005) nhấn mạnh, tác giả lập luận rằng khả năng quản lý rủi ro hiệu quả của một tổ chức bắt nguồn từ khả năng quản lý kiến thức liên quan.

Liên quan đến an ninh mạng, Tisdale (2015) nêu ra sự cần thiết của các phương pháp tiếp cận đa chiều nhằm mở rộng triển vọng kỹ thuật điển hình, ủng hộ định hướng hệ thống, độ phức tạp và nền tảng quản lý tri thức. Trong bối cảnh bảo mật Thông tin, Shedden & cộng sự (2011) minh họa tầm quan trọng của việc tính toán các rủi ro đối với việc trau dồi và triển khai kiến thức về tổ chức.

Hình 1. Các thành phần của quản lý rủi ro



(Nguồn: Whitman & Mattord, 2014)

Xác định rủi ro là vấn đề đầu tiên không liên quan trực tiếp đến công nghệ, nhưng là tiền thân quan trọng để thực hiện các biện pháp kiểm soát công nghệ. Dữ liệu là tài sản quan trọng nhất, nếu bị mất hoặc bị xâm phạm, sẽ khiến tổ chức bị thiệt hại đáng kể hoặc thậm chí có thể đe dọa sự tồn tại của tổ chức. Do đó, xác định cụ thể dữ liệu, thông tin kế toán quan trọng nhất là một công việc quan trọng. Sau khi dữ liệu, thông tin kế toán quan trọng được xác định, mức độ bảo mật cao nhất có thể được hướng đến các quy trình và hệ thống thu thập, lưu trữ và duy trì dữ liệu kế toán này, trong khi các biện pháp bảo mật ít nghiêm ngặt hơn và ít tốn kém hơn có thể được áp dụng cho dữ liệu, thông tin không quan trọng.

Để xác định dữ liệu kế toán này, bạn hãy bắt đầu bằng cách hỏi những người chủ chốt trong tổ chức của bạn về dữ liệu nào là thực sự cần thiết (hoặc nhiệm vụ quan trọng). Bạn sẽ thấy rằng dữ liệu quan trọng thường được liên kết với các khía cạnh của tổ chức xác định tính độc nhất của tổ chức và tạo ra tính cạnh tranh thuận lợi. Dữ liệu quan trọng cũng thường được liên kết với các nguồn lực thiết yếu (như hàng tồn kho hoặc tiền mặt) và các nhóm bên liên quan chính

(chẳng hạn như khách hàng, nhà cung cấp và nhân viên). Ngoài ra, cần suy nghĩ về các quy trình kinh doanh cốt lõi trong tổ chức của bạn, chẳng hạn như chu trình doanh thu và chu trình chi phí. Bởi lẽ các quy trình này là trọng tâm của một tổ chức, chúng thường sẽ tạo ra khối lượng lớn dữ liệu và nếu hệ thống tạo ra dữ liệu không thành công, sẽ dẫn đến chi phí thời gian ngừng hoạt động cao, đây là hai đặc điểm chính của các hệ thống quan trọng.

Một khía cạnh khác của dữ liệu quan trọng là nó thường được tạo ra bởi các quá trình tích hợp hoặc hợp nhất tồn tại ở giao điểm của các mô-đun nghiệp vụ. Tại các điểm tích hợp, dữ liệu từ các bộ phận khác nhau của tổ chức hợp nhất, sẽ tạo ra nhiều thông tin được các nhà quản lý thực hiện quyết định đánh giá cao.

4. Nâng cao văn hóa nhận thức an ninh mạng

Khi tổ chức đã xác định các chính sách hướng dẫn chương trình an toàn và chọn mô hình an toàn tổng thể bằng cách tạo, điều chỉnh bảng kế hoạch chi tiết tương ứng, bước tiếp theo cần triển khai chương trình giáo dục, huấn luyện và nâng cao nhận thức về an toàn, hay còn gọi là chương trình SETA). Chương trình SETA phải do giám đốc an toàn thông tin (CISO) phụ trách và là một biện pháp kiểm soát được thiết kế để giảm các sự cố do nhân viên vô tình vi phạm an ninh. Lỗi của nhân viên là một trong những mối đe dọa hàng đầu đối với tài sản thông tin, do đó, phát triển chương trình SETA để chống lại mối đe dọa này là cần thiết. SETA được thiết kế để bổ sung cho các chương trình giáo dục và huấn luyện chung mà nhiều tổ chức sử dụng để huấn luyện nhân viên về an ninh mạng. Mục đích của SETA là tăng cường an toàn bằng cách thực hiện những điều sau:

- Nâng cao nhận thức về sự cần thiết phải bảo vệ tài nguyên hệ thống
- Phát triển kỹ năng và kiến thức để người dùng máy tính có thể thực hiện công việc của họ một cách an toàn hơn
- Xây dựng kiến thức chuyên sâu khi cần thiết để thiết kế, triển khai hoặc vận hành các chương trình an toàn cho các tổ chức và hệ thống

Bảng 1. Khuôn mẫu so sánh của chương trình SETA

	Giáo dục	**Huấn luyện**	**Nâng cao nhận thức**
Thuộc tính	Tại sao	Như thế nào	Cái gì
Cấp độ	Bản chất (Insight)	Kiến thức	Thông tin
Mục tiêu	Hiểu	Kỹ năng	Sự trình bày
Phương pháp giảng dạy	Hướng dẫn lý thuyết - Thảo luận	Hướng dẫn thực hành	Phương tiện truyền thông

	- Đọc kiến thức - Thực hành	- Bài giảng - Tình huống - Posters	- Videos - Newletters
Biện pháp kiểm tra	Bài luận	Giải quyết vấn đề	Trắc nghiệm
Khung thời gian ảnh hưởng	Dài hạn	Trung hạn	Ngắn hạn

(Nguồn: NIST SP 800-12)

Cụ thể cần làm việc với bộ phận công nghệ thông tin của bạn để tạo một trang web nâng cao nhận thức về an ninh mạng nhằm giáo dục nhân viên về các rủi ro an ninh mạng. Bao gồm chính sách an ninh mạng của bạn, giải thích về các vấn đề và các báo cáo báo chí gần đây về vi phạm an ninh mạng. Việc hiểu rõ rủi ro và chiến thuật "sói đội lốt cừu" mà tin tặc sử dụng sẽ giúp người dùng nhạy bén hơn với phản xạ để nhanh chóng xác định, phản ứng, ngăn chặn và chặn đứng các cuộc tấn công. Thời gian là tiền bạc trong cuộc chiến tranh mạng. Xây dựng chương trình đào tạo có ý nghĩa và hiệu quả để phát triển các nhân viên chuyên nghiệp về an ninh mạng.

Tăng cường đào tạo với liên lạc liên tục xác định các mối đe dọa hiện tại và cách đối phó. Ví dụ: Đại học Kinh tế TP.HCM thông báo cho cộng đồng của mình qua email khi phát hiện thấy một email spam hoặc lừa đảo và hướng dẫn người dùng xóa email ngay lập tức. Chia sẻ các chiến lược để xác định và bảo vệ người dùng từ các email lừa đảo như khuyến khích nhân viên tạo mật khẩu mạnh và duy nhất và báo cáo ngay các email đáng ngờ cho bộ phận công nghệ thông tin cũng như không khuyến khích cả việc chia sẻ mật khẩu và cung cấp thông tin ngay lập tức theo yêu cầu.

5. Áp dụng kiến thức quản trị an ninh mạng

Nhiều nhân viên kế toán quản trị tích cực tham gia vào việc phát triển, thực hiện và giám sát kiểm soát nội bộ của tổ chức họ bằng cách sử dụng Khuôn mẫu Kiểm soát nội bộ tích hợp của COSO. Các tổ chức phải mở rộng các biện pháp kiểm soát nội bộ để chống lại các mối đe dọa an ninh mạng bằng quản trị an ninh mạng. Các khái niệm và quy trình để áp dụng khuôn mẫu an ninh mạng được xây dựng dựa trên các kỹ năng và công cụ học được từ việc triển khai khuôn mẫu COSO. Một số khuôn mẫu quản trị an ninh mạng được sử dụng rộng rãi giải quyết rủi ro an ninh mạng, bao gồm Khuôn mẫu an ninh mạng của Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) của Bộ Thương mại Hoa Kỳ và ISO 27000.

Khung CSF bao gồm ba thành phần: cốt lõi, cấu hình và các cấp triển khai. Phần cốt lõi bao gồm các kết quả an ninh mạng phi kỹ thuật rõ ràng, có thể dễ dàng điều chỉnh cho phù hợp với

một tổ chức: xác định, bảo vệ, phát hiện, phản ứng và phục hồi. Phần cấu hình đề cập đến các yêu cầu, mục tiêu, mức độ chấp nhận rủi ro và những nguồn lực cụ thể của một tổ chức, trong khi phần các cấp triển khai đề cập đến cách thức tổ chức quản lý rủi ro an ninh mạng bao gồm ba yếu tố cần hướng đến của an toàn thông tin: tính bảo mật, tính toàn vẹn và tính khả dụng.

6. Triển khai vị trí Giám đốc an toàn thông tin (CISO)

Các tổ chức phải chủ động quản lý các rủi ro và mối đe dọa an ninh mạng. Bảo vệ một tổ chức là một trách nhiệm được chia sẻ bắt đầu từ ban giám đốc và xuyên suốt tổ chức. Nếu rủi ro xảy ra, tổ chức phải chịu trách nhiệm. Hãy nhớ rằng, rủi ro an ninh mạng không chỉ là rủi ro của bộ phận công nghệ thông tin mà là rủi ro cho mọi nhân viên, nhà quản lý, đối tác kinh doanh đều sở hữu rủi ro. Khuôn mẫu COBIT 2019 xác định cơ cấu tổ chức là một yếu tố quan trọng để đạt được các biện pháp kiểm soát hiệu quả và bảo mật. Điều đặc biệt quan trọng là các tổ chức giao trách nhiệm về thông tin bảo mật cho một cấp quản lý cấp cao thích hợp vì như vậy tổ chức sẽ có nhiều khả năng có một nhóm ứng phó sự cố được đào tạo tốt hơn so với các tổ chức không bắt một người nào đó chịu trách nhiệm về bảo mật thông tin. Và một cách để đáp ứng mục tiêu này là tạo ra vị trí CISO, vị trí này nên độc lập với các chức năng hệ thống thông tin khác và nên báo cáo cho giám đốc hoạt động (COO) hoặc giám đốc điều hành (CEO). CISO phải hiểu môi trường công nghệ của công ty và làm việc với giám đốc thông tin (CIO) để thiết kế, thực hiện và thúc đẩy các chính sách và quy trình bảo mật hợp lý. CISO cũng nên là một người xem xét và đánh giá khách quan về môi trường công nghệ thông tin. Theo đó, CISO phải có trách nhiệm đảm bảo rằng các đánh giá lỗ hổng và rủi ro được thực hiện thường xuyên và kiểm toán bảo mật được thực hiện định kỳ. CISO cũng cần hợp tác chặt chẽ với người phụ trách an ninh vật lý vì truy cập vật lý trái phép có thể cho phép kẻ xâm nhập vượt qua các kiểm soát truy cập logic phức tạp nhất. Do đó, đây là một vị trí giám đốc cấp cao chịu trách nhiệm về bảo mật công nghệ thông tin, từ xác định rủi ro an ninh mạng đến dẫn đầu phản ứng đối với vi phạm dữ liệu, CISO nên bao gồm việc liên lạc viên với công nghệ thông tin, kế toán và tài chính, hoạt động, tiếp thị và bán hàng.

Tài liệu tham khảo

Brands, K., & Elam, D. (2021). Strategies for Crisis Management in a Pandemic: A Framework for Businesses and Organisations. *The New Normal: Challenges of Managing Business, Social and Ecological Systems in the Post COVID 19 Era*.

Gordon, L. A., & Loeb, M. P. (2006). Budgeting process for information security expenditures. *Communications of the ACM*, *49*(1), 121-125.

Max-Neef, M. A. (2005). Foundations of transdisciplinarity. *Ecological economics*, *53*(1), 5-16.

No, W. G., & Vasarhelyi, M. A. (2017). Cybersecurity and continuous assurance. *Journal of Emerging Technologies in Accounting*, *14*(1), 1-12.

Sallos, M. P., Garcia-Perez, A., Bedford, D., & Orlando, B. (2019). Strategy and organisational cybersecurity: a knowledge-problem perspective. *Journal of Intellectual Capital*.

Shedden, P., Scheepers, R., Smith, W., & Ahmad, A. (2011). Incorporating a knowledge perspective into security risk assessments. *Vine*.

Starr, S., Kuehl, D., & Pudas, T. (2010). Perspectives on building a cyber force structure. In *Proc. Conf. on Cyber Conflict*, 163-181.

Tisdale, S. M. (2015). Cybersecurity: Challenges from a Systems, Complexity, Knowledge Management and Business Intelligence Perspective. *Issues in Information Systems*, *16*(3).

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.

Whitman, M., & Mattord, H. J. (2014). Information security governance for the non-security business executive.

Trang web: https://csrc.nist.gov/publications/detail/sp/800-12/rev-1/final

Trang web: https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Luat-an-ninh-mang-2018-351416.aspx