Tạp chí Nghiên cứu Kinh tế và Kinh doanh Châu Á
Năm thứ 34, Số 11 (2023), 122–137

www.jabes.ueh.edu.vn

JABES
Tạp chí Nghiên cứu Kinh tế và Kinh doanh Châu Á

Tạp chí Nghiên cứu Kinh tế và Kinh doanh Châu Á
http://www.emeraldgrouppublishing.com/services/publishing/jabes/

Mô hình văn hóa an toàn thông tin kế toán: Một nghiên cứu thực nghiệm tại Việt Nam

PHẠM TRÀ LAM [a, *], ĐẬU THỊ KIM THOA [a], NGUYỄN PHƯỚC BẢO ẤN [a]

[a] *Đại học Kinh tế Thành phố Hồ Chí Minh*

THÔNG TIN

Ngày nhận: 11/05/2023
Ngày nhận lại: 08/08/2023
Duyệt đăng: 08/08/2023

Mã phân loại JEL:
I32; O13.

Từ khóa:
Văn hóa an toàn thông tin;
Hành vi an toàn thông tin;
An toàn thông tin kế toán.

Keywords:
Information Security Culture;
Information Security Behavior;
Accounting Information Security.

TÓM TẮT

Trong thế giới kỹ thuật số phức tạp, nhiều doanh nghiệp đã đầu tư vào các công nghệ an toàn tiên tiến và các cơ chế khác hỗ trợ cho mục đích an toàn thông tin (Information Security – IS), đặc biệt là thông tin kế toán, bởi sự gia tăng về độ phức tạp và các loại nguy cơ ngày càng gia tăng và biến động không ngừng. Phát triển văn hóa an toàn thông tin (Information Security Culture – ISC) được xem là một biện pháp mang tính hiệu quả cao. Do đó, nghiên cứu này đã phát triển một mô hình cấu trúc gồm các yếu tố của ISC đó là thái độ, nhận thức, năng lực và hành vi an toàn thông tin (Information Security Behavior – ISB). Dữ liệu thu thập từ 181 nhân viên đang đảm nhiệm các công việc liên quan đến kế toán và IS được phân tích bằng kỹ thuật PLS chứng minh rằng nhận thức và năng lực IS chi phối mạnh đến định hướng hành vi an toàn thông tin (Behavior Intention – BI) của nhân viên. Các cấu trúc này của ISC tạo ra những đóng góp đáng kể đến ISB. Những khám phá này đã cung cấp những hiểu biết mới về các yếu tố của ISC, đóng góp cho các nhà quản trị các hàm ý nhằm đạt được các mục tiêu IS kế toán.

Abstract

In the complex digital world, businesses have invested in advanced security technologies and other mechanisms that support information security (IS), especially accounting information security, because of the increasing ramifications and diversity of threats, which are increasing and changing constantly. Building an information security culture (ISC) is considered a highly effective approach. Therefore, this study developed a structural model including the four dimensions of ISC

[*] Tác giả liên hệ.
Email: phamtralamais@ueh.edu.vn (Phạm Trà Lam), kimthoa@ueh.edu.vn (Đậu Thị Kim Thoa), baoan@ueh.edu.vn (Nguyễn Phước Bảo Ấn)

Trích dẫn bài viết: Phạm Trà Lam, Đậu Thị Kim Thoa, & Nguyễn Phước Bảo Ấn. (2023). Mô hình văn hoá an toàn thông tin kế toán: Một nghiên cứu thực nghiệm tại Việt Nam. *Tạp chí Nghiên cứu Kinh tế và Kinh doanh Châu Á, 34*(11), 122–137.

which are accounting IS attitudes, awareness, competencies, and behavior (ISB). Data collected from 181 employees are analyzed by the PLS proving that information security awareness and competencies strongly impact behavior intention. These structures of the ISC create significant contributions to the ISB. The findings provide new insights about ISC, providing managers with implications for successful accounting information security.

1. Giới thiệu

Cuộc cách mạng công nghiệp 4.0 với những phát triển vượt bậc về công nghệ thông tin và truyền thông (Information and Communication Technologies – ICTs) đã mang lại những thay đổi tích cực trong hoạt động kinh doanh và lợi thế cạnh tranh. Song nó cũng tạo ra nhiều thách thức và rủi ro cho doanh nghiệp (Taiwo, 2016). Một trong những mối đe doạ nghiêm trọng mang tính toàn cầu mà các doanh nghiệp phải đối mặt là vấn đề an toàn thông tin (Information Security – IS) (Bawaneh, 2014). Theo Báo cáo kinh doanh an ninh mạng, tội phạm mạng được tin rằng đã gây thiệt hại "hơn 6 nghìn tỷ USD vào năm 2021, tăng từ 3 tỷ USD vào năm 2015" (Khando và cộng sự, 2021). Do đó, việc bảo đảm IS để thích ứng một cách sáng tạo với những tiến bộ của ICTs đang trở thành một vấn đề ưu tiên hàng đầu của các doanh nghiệp (Khando và cộng sự, 2021).

Với những ưu điểm vượt trội của ICTs, hầu hết các hoạt động kinh tế tại các doanh nghiệp đều sử dụng hệ thống thông tin trên máy vi tính. Đặc biệt, ICTs cũng đã ảnh hưởng đáng kể đến lĩnh vực kế toán (Al-Fatlawi và cộng sự, 2021). Hệ thống thông tin kế toán (Accounting Information System – AIS) trên máy vi tính và các công cụ kế toán quản trị do công nghệ thông tin (CNTT) cung cấp được các doanh nghiệp ứng dụng ở các mức độ khác nhau. Tuy nhiên, AIS cũng đang phải đối mặt với nhiều nguy cơ bị tấn công và các vấn đề IS (Al-Fatlawi và cộng sự, 2021). Trước bối cảnh này, phần lớn các giải pháp kỹ thuật được các doanh nghiệp triển khai dựa vào các công nghệ IS và kiểm soát con người trong hệ thống (Ngo và cộng sự, 2005). Tuy nhiên, các cơ chế IS tốt cần giải quyết cả khía cạnh kỹ thuật và phi kỹ thuật (Ali và cộng sự, 2021). Do đó, trọng tâm là thiết lập văn hóa an toàn thông tin (Information Security Culture – ISC) tại các doanh nghiệp (Zakaria và cộng sự, 2007).

ISC là một thành phần của văn hoá doanh nghiệp (Uchendu và cộng sự, 2021), nó sẽ phát triển và thành công khi có sự tham gia của tất cả nhà quản trị và nhân viên. Nhân viên cần nhận thức được các mối đe dọa an toàn tiềm ẩn đối với tổ chức, đặc biệt là các sự cố IS nội bộ (Zakaria và cộng sự, 2007). Điều này liên quan đến việc thay đổi hành vi, thái độ, và nhận thức của mọi người để có nhận thức và hiểu biết về IS (Khando và cộng sự, 2021).

ISC là một lĩnh vực nghiên cứu mới nổi và cho đến hiện tại nó được giải thích bằng nhiều lý thuyết và nguyên tắc được thiết lập từ nhiều lĩnh vực nghiên cứu khác như lý thuyết hành động hợp lý (Theory of Reasoned Action – TRA) (Fishbein & Ajzen, 1975) và mô hình chấp nhận công nghệ (Technology Acceptance Model – TAM) (Davis, 1989). Các nghiên cứu hiện hành về ISC đa phần được thực hiện ở các nước phát triển (Marks, 2007). Trong khi ở các nước đang phát triển, môi trường văn hoá xã hội cùng với việc thiếu nguồn lực và kiến thức đang tạo ra nhiều rào cản lớn trong việc thúc đẩy nhận thức về IS nhưng vẫn chưa nhận được nhiều sự quan tâm từ các nhà nghiên cứu (Rezgui

& Marks, 2008). Tại Việt Nam, việc vận dụng ICTs vào AIS khá được chú trọng trong thời gian qua. Tuy nhiên, vấn đề nghiên cứu về IS trong kế toán vẫn còn rất hạn chế. Do đó, nghiên cứu này tập trung vào ISC, một giải pháp quan trọng cho mục tiêu IS kế toán. Những phát hiện của nghiên cứu này sẽ giúp nhà quản trị có sự hiểu biết sâu sắc hơn về vai trò của ISC và mối quan hệ giữa các thành phần ISC trong AIS. Trên cơ sở đó, doanh nghiệp có thể xây dựng các chiến lược và chính sách nâng cao ISC và ISB.

Phần tiếp theo của bài viết trình bày cơ sở lý thuyết, phương pháp nghiên cứu, kết quả nghiên cứu, thảo luận, và hàm ý nghiên cứu. Cuối cùng, các kết luận của nghiên cứu được tổng hợp.

2. Cơ sở lý thuyết

2.1. Văn hoá an toàn thông tin và Hệ thống thông tin kế toán

2.1.1. Văn hoá an toàn thông tin (Information Security Culture – ISC)

ISC được hiểu là một văn hóa an toàn và bảo mật thông tin lý tưởng, mọi nhân viên tuân theo các hướng dẫn một cách tự nguyện theo cách thức khiến nó trở thành bản chất tự nhiên thứ hai của họ (Vroom và von Solms, 2004). Theo Zakaria và cộng sự (2007), ba đặc điểm chung của ISC bao gồm: (1) định hình hành vi của nhân viên hướng đến sự quan tâm về an toàn, (2) tạo ra một môi trường an toàn trong một tổ chức, và (3) yêu cầu sự tham gia của tất cả nhân viên. ISC được xem là các giả định về các ISB được chấp nhận và được khuyến khích đến các nhân viên của tổ chức (Ngo và cộng sự, 2005). Chất lượng của ISC được xác định bởi niềm tin của tổ chức và bằng cách đánh giá và quản lý nguyên tắc tôn trọng sự thật cũng như tính hợp lý trong niềm tin của người dùng cuối và nhà quản trị đối với IS của tổ chức (Ruighaver và cộng sự, 2007).

Từ khía cạnh thực tiễn, ISC là một yếu tố quan trọng để chống lại rủi ro liên quan đến con người. Theo da Veiga và cộng sự (2020) tổng hợp, tổ chức hợp tác và phát triển kinh tế (Organisation for Economic Co-operation and Development – OECD) đã công bố Hướng dẫn An toàn cho Hệ thống Thông tin và Mạng với trọng tâm là xây dựng ISC. Tương tự, các tác giả da Veiga và cộng sự (2020) tổng hợp cũng đề cập rằng Đại hội đồng Liên Hợp Quốc (2003) đã giới thiệu một tài liệu có tiêu đề "Tạo ra văn hóa an toàn mạng toàn cầu". Hiện tại, có nhiều khuôn mẫu về IS như ISO 27000[1], NIST và an toàn[2], COBIT[3], COSO[4] (Whitman & Mattord, 2016); cung cấp các hướng dẫn về chương trình giáo dục, đào tạo và nâng cao nhận thức IS (Security Education, Training, and Awareness – SETA) và các chính sách, cơ chế IS để giải quyết yếu tố con người.

Georgiadou và cộng sự (2020) đã tổng hợp và xác nhận ISC có hai cấp độ tổ chức và cá nhân. Trong nghiên cứu này, nhóm tác giả quan tâm đến ISC từ các khía cạnh cá nhân gồm "Thái độ", "Hành vi", "Năng lực", và "Nhận thức". Trong đó, khía cạnh "Thái độ" đề cập đến cảm xúc và niềm

[1] ISO 27000 là một tiêu chuẩn về hệ thống quản lý an toàn thông tin (Information Security Management Systems – ISMS)

[2] NIST và an toàn bao gồm các mô hình về an toàn thông tin do Viện Tiêu chuẩn và Công nghệ Quốc gia của Hoa Kỳ ban hành (National Institute of Standards and Technology – NIST) bao gồm các khuôn mẫu như SP 800-12, Rev. 1, SP 800-18, Rev. 1, SP 800-30, Rev. 1, SP 800-37, Rev. 2

[3] COBIT là khuôn mẫu về kiểm soát và công nghệ với tiêu đề là mục tiêu kiểm soát đối với công nghệ thông tin (Control Objectives for Information Technologies – COBIT) được ban hành bởi Hiệp hội kiểm toán và kiểm soát hệ thống thông tin (Information Systems Audit and Control Association – ISACA) có trụ sở chính tại Hoa Kỳ

[4] COSO là Ủy ban các tổ chức tài trợ (Committee of Sponsoring Organizations – COSO) của Hoa Kỳ đã ban hành nhiêu khuôn mẫu kiểm soát và quản trị rủi ro như phiên bản kiểm soát nội bộ 1992, kiểm soát nội bộ 2013, quản trị rủi ro doanh nghiệp 2003

tin của nhân viên đối với các giao thức và các vấn đề an toàn. Khía cạnh "Hành vi" gồm các chính sách, thủ tục, và sự tuân thủ. Yếu tố "Năng lực" trong ISC liên quan đến những khả năng, kỹ năng, kiến thức, và chuyên môn của nhân viên về IS, cho phép họ tuân thủ các chính sách và quy trình bảo mật của tổ chức. Nhận thức về an toàn thông tin (Information Security Awareness – ISAW) là một yếu tố quan trọng của ISC bởi ISAW đề cập đến mức độ mà nhân viên hiểu rõ tầm quan trọng của các chính sách, quy tắc và hướng dẫn IS của tổ chức. ISAW cũng được xem là mức độ mà nhân viên hành xử theo các chính sách, quy tắc và hướng dẫn về IS của tổ chức (Siponen, 2000). Theo Georgiadou và cộng sự (2021), nhận thức về chính sách, thủ tục và nhận thức về vai trò, trách nhiệm là hai thành tố của ISAW. Nhiều học giả cho rằng việc thiết lập ISC sẽ làm giảm các mối đe dọa nội bộ đối với an ninh thông tin, chẳng hạn như Alfawaz và cộng sự, 2010; Furnell và Rajendran, 2012; da Veiga, 2018; và da Veiga và cộng sự, 2020).

2.1.2. Hệ thống thông tin kế toán (Accounting Information System – AIS)

AIS là một hệ thống con được tích hợp thông tin từ các hệ thống con khác nhau của nó và truyền thông tin này đến các hệ thống con xử lý thông tin của tổ chức để hỗ trợ các nhà quản lý trong việc ra quyết định (Simkin và cộng sự, 2014). Ngày nay các AIS quan tâm nhiều đến các dữ liệu và thông tin tài chính và phi tài chính (Dandago & Rufai, 2014). Trong bối cảnh của thế giới số, nhiều doanh nghiệp phát triển AIS trên nền máy vi tính và sử dụng nhiều công cụ kế toán quản trị với sự hỗ trợ của ICTs.

Bên cạnh những ưu việt của ICTs, những công nghệ này có thể tạo ra một môi trường không an toàn vì hiệu quả của chúng phụ thuộc rất nhiều vào cách chúng được thực hiện trong tổ chức (Alhogail & Mirza, 2014). Do đó, các khía cạnh kiểm soát và an toàn AIS ngày càng trở thành mối quan tâm của cả doanh nghiệp và cộng đồng khoa học (Almagtome và cộng sự, 2020). Nhân viên hiện tại được đánh giá là nguồn gây ra sự cố IS cao nhất, tiếp theo là những nhân viên cũ của tổ chức. Các vấn đề về IS thường liên quan đến sự bất cẩn hoặc lỗi của con người (Ponemon, 2018). Như vậy, các tổ chức đều có mong muốn phát triển các kỹ năng cần thiết cho nhân viên và thu hút sự quan tâm của họ vào quá trình thực hiện IS thông qua việc xây dựng và phát triển ISC (Ghafir và cộng sự, 2018).

Các tổng quan nghiên cứu cho thấy phần lớn các nghiên cứu trước tập trung vào vấn đề IS nói chung. Trong khi, những tác động của ICTs đối với AIS ngày càng gia tăng và kéo theo các vấn đề về IS kế toán. Do đó, trong nghiên cứu này, nhóm tác giả chọn phạm vi nghiên cứu là IS cho các AIS được tin học hóa.

2.2. Mô hình hành vi thái độ nhận thức và Văn hoá an toàn thông tin

Theo mô hình hành vi thái độ nhận thức (Knowledge-Attitude-Behavior – KAB), kiến thức, thái độ, và hành vi của con người có mối quan hệ với nhau. Kiến thức là sự hiểu biết của một người về một lĩnh vực cụ thể, có vai trò quan trọng tác động đến thái độ và hành vi của con người. Thái độ thể hiện nhận thức tích cực hoặc tiêu cực của cá nhân về việc thực hiện một hành vi. Hành vi là những hành động được thực hiện dựa trên kiến thức và thái độ. Nó phản ánh cách mà con người ứng dụng kiến thức và thái độ của mình vào thực tế (Schrader & Lawless, 2004). Dựa vào KAB, Parsons và cộng sự (2014) đã xác nhận khi kiến thức của nhân viên về IS tăng lên, thái độ của họ được cải thiện, dẫn đến ISB được cải thiện.

Phát triển từ KAB, nhiều nghiên cứu đã chứng minh rằng các yếu tố của ISC có mối quan hệ với nhau. Cichowicz và cộng sự (2021) lập luận rằng có tồn tại mối quan hệ tích cực giữa nhận thức về

rủi ro mạng và ISB trong thế giới mạng. Nhận thức về an toàn mạng của nhân viên liên quan đến các sự cố an ninh mạng (Wang và cộng sự, 2022). Bằng cách tổ chức đào tạo nâng cao nhận thức, tác động của nó đến kiến thức, thái độ và hành vi của nhân viên đã được xác nhận (Sas và cộng sự, 2021). Theo Khando và cộng sự (2021), ISAW của nhân viên trở đã thành một trong những khía cạnh quan trọng của việc bảo vệ chống lại ISB không mong muốn. Bên cạnh đó, Parsons và cộng sự (2014) đã tìm thấy mối quan hệ tích cực giữa ISA và ISC. Nhân viên từ các tổ chức có ISC tốt có nhiều khả năng có kiến thức, thái độ và hành vi phù hợp với các chính sách và quy trình IS cần thiết để duy trì IS tốt trong tổ chức (D'Arcy & Greene, 2014).

Kết hợp các nghiên cứu trên cùng với lý thuyết TRA và TAM, nhóm nghiên cứu giả định ISAW ảnh hưởng đến BI; từ đó, sẽ ảnh hưởng đến ISB của nhân viên trong AIS. Theo Ajzen (1991), ý định bao gồm các yếu tố động cơ ảnh hưởng đến hành vi, là dấu hiệu cho thấy một cá nhân sẵn sàng cố gắng đến mức nào, họ dự định nỗ lực đến mức nào để thực hiện hành vi. Trong bối cảnh này, chúng tôi định nghĩa BI là mức độ cố gắng hay nỗ lực của nhân viên để thực hiện ISB. Dựa trên các lập luận trên, nhóm tác giả phát triển giả thuyết:

H_1: ISAW có ảnh hưởng tích cực đến BI.

Thái độ được hiểu là niềm tin liên quan đến hậu quả của hành vi, và chuẩn chủ quan hay ảnh hưởng của xã hội bao gồm niềm tin quy chuẩn và động lực tuân thủ (Fishbein & Ajzen, 1975). Thái độ đối với an toàn của nhân viên trong các cơ quan công quyền có ảnh hưởng đến ISB (Townsend III, 2022). Hadlington và Murphy (2018) đã phát hiện thái độ về hành vi có liên quan tích cực đến các hoạt động an ninh mạng.

Theo Sánchez-Caballé và cộng sự (2020), kiến thức của cá nhân là thông tin, sự hiểu biết và kỹ năng mà cá nhân đó đạt được thông qua giáo dục hoặc trải nghiệm. Ricci và cộng sự (2019) khẳng định, đào tạo để nâng cao năng lực IS là điều cần thiết đối với tất cả người dùng Internet để bảo vệ khỏi các hành vi lừa đảo và mất dữ liệu trực tuyến. Nghiên cứu gần đây của Yaokumah và cộng sự (2019) cho thấy tính hiệu quả của SETA bị ảnh hưởng bởi thái độ của nhân viên. Các học giả đã tiến hành các nghiên cứu tổng hợp lý thuyết và chứng thực những tác động khác nhau của thái độ, nhận thức, năng lực IS đến ISB trong nhiều bối cảnh khác nhau (Sulaiman và cộng sự, 2022). Theo KAB, kiến thức ảnh hưởng tích cực đến ISB. Bởi vì kiến thức là nền tảng cơ bản tạo ra năng lực (Westera, 2001), năng lực IS được tạo ra từ các kiến thức về IS.

Parsons và cộng sự (2014) đã nhận định ISC thông qua nhân viên có thể trở thành cơ chế bảo vệ mạnh mẽ nhất trước các mối đe dọa IS. Theo Warkentin và cộng sự (2016), sự tham gia liên tục của một cá nhân vào các hành vi bảo vệ an toàn là quan trọng trong việc đảm bảo IS. Ali và cộng sự (2021) xác nhận các thành phần trong ISC và một số yếu tố khác như các kỹ thuật ngăn chặn, hành vi quản lý, xung đột giá trị, căng thẳng liên quan đến an ninh, sự trung lập, động lực bên trong và bên ngoài, và sự bảo vệ đóng vai trò quan trọng đối với các ISB. Do đó, ISC hỗ trợ tăng cường kết quả hoạt động của tổ chức. Trong nghiên cứu này, nhóm tác giả kết hợp lý thuyết TRA, TAM, KAB và các nghiên cứu trước để phát triển các giả thuyết:

H_2: Thái độ an toàn thông tin (ISA) có ảnh hưởng tích cực đến BI.

H_3: Năng lực IS có ảnh hưởng tích cực đến BI.

Theo lý thuyết nguồn lực (RBV), ISC được xem là một nguồn lực duy nhất, đặc biệt của một doanh nghiệp. RBV cho rằng khả năng cạnh tranh vững chắc đến từ các tài sản hữu hình và vô hình

độc đáo có giá trị, khan hiếm, không thể bắt chước hoàn toàn và bền vững (Peteraf, 1993). Nhiều học giả đồng tình ISC là một tài sản đặc biệt của tổ chức (Georgiadou và cộng sự, 2021; Gioulekas và cộng sự, 2022). Dựa vào các lý thuyết hành vi, các nghiên cứu trước đây về mối quan hệ giữa thái độ IS và ISB đã được xác nhận (Sas và cộng sự, 2021; Wang và cộng sự, 2022). Kết hợp KAB và công trình nghiên cứu của một số học giả như Ricci và cộng sự (2019) và Sulaiman và cộng sự (2022), năng lực IS có tác động đến ISB. Như vậy, dựa trên sự kết hợp của KAB, RBV, các lý thuyết hành vi và một số nghiên cứu, nhóm tác giả phát triển các giả thuyết:

H_4: BI có ảnh hưởng tích cực đến ISB.

H_5: ISA có ảnh hưởng tích cực đến ISB.

H_6: Năng lực IS có ảnh hưởng tích cực đến ISB.

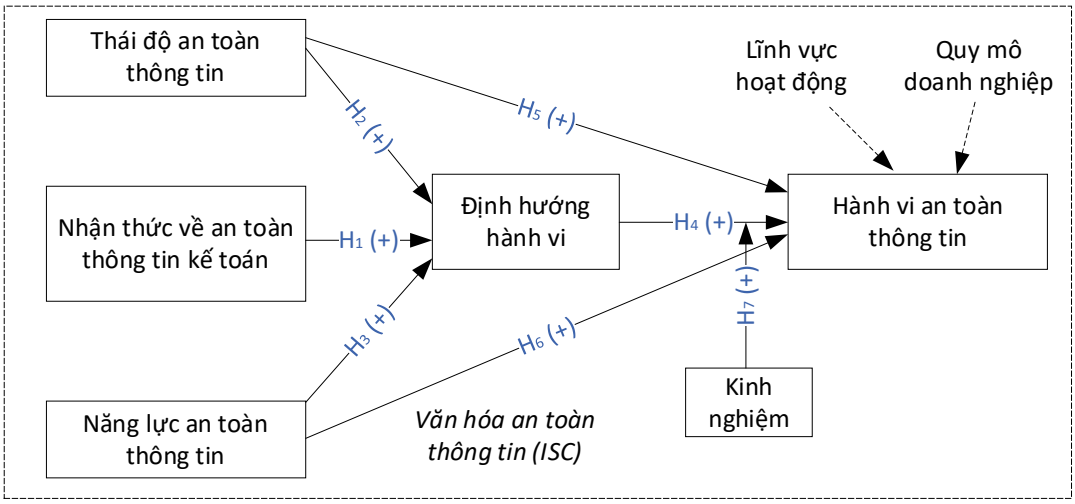
2.3. Vai trò điều tiết của kinh nghiệm

Theo Haeussinger và Kranz (2013), những trải nghiệm tiêu cực trước đây với các sự cố IS khiến ISAW của nhân viên được cải thiện. Hwang và cộng sự (2019) cũng xác nhận mối liên hệ giữa kinh nghiệm trong quá khứ về IS và ISAW của nhân viên. ISAW không chỉ là nhận thức có ý thức về các kích thích trong trải nghiệm hiện tại mà còn là sự xuất hiện của quá khứ, hiện tại và tương lai (Khando và cộng sự, 2021). Humaidi và Balakrishnan (2015) đã chỉ ra kinh nghiệm làm việc của nhân viên y tế tạo ra tác động điều tiết đối với hành vi tuân thủ chính sách IS thông tin y tế. Do đó, kinh nghiệm của về IS trong quá khứ và hiện tại sẽ đóng góp cho ISB.

Trong mô hình TAM3, yếu tố kinh nghiệm của người sử dụng hệ thống đóng vai trò điều tiết cho nhiều mối quan hệ như: chuẩn chủ quan, sự lo sợ về máy tính, cảm nhận về tính hữu ích, cảm nhận về tính dễ sử dụng… với ý định hành vi chấp nhận công nghệ (Venkatesh & Bala, 2008). Trong tình huống này, dựa vào một số nghiên cứu thực nghiệm nhận định về tác động của kinh nghiệm đến hành vi chấp nhận công nghệ (McFarland & Hamilton, 2006; Poon, 2008), các nghiên cứu về tác động của kinh nghiệm đến một số yếu tố của ISC và TAM3, nhóm tác giả phát triển giả thuyết:

H_7: Kinh nghiệm về IS điều tiết tác động của BI đến ISB.

Trong nghiên cứu này, chúng tôi dự đoán ISB là khác biệt theo quy mô doanh nghiệp, do đó, để loại bỏ tác động gây nhiễu của quy mô đến ISB (nếu có), quy mô được xem là biến kiểm soát (Huzaizi và cộng sự, 2021). Theo Gioulekas và cộng sự (2022), các tổ chức hoạt động trong các lĩnh vực khác nhau có thể sẽ có ISB khác biệt, vì vậy, lĩnh vực cũng được xem là biến kiểm soát.



Hình 1. Mô hình nghiên cứu

3. Phương pháp nghiên cứu

3.1. Đo lường

Nghiên cứu này chấp nhận thang đo từ các nghiên cứu trước có điều chỉnh cho phù hợp với bối cảnh nghiên cứu trong AIS. Các đối tượng tham gia khảo sát được yêu cầu cho biết mức độ đồng ý theo thang đo Likert 7 điểm, từ 1 (hoàn toàn không đồng ý/ hoàn toàn không có) đến 7 (hoàn toàn đồng ý/ hoàn toàn có). ISA, ISAW, năng lực IS (ISCO), và ISB được đo lường theo đề xuất của Georgiadou và cộng sự (2021). ISA gồm ba thành phần đo lường: thái độ, hồ sơ, và sự hài lòng của nhân viên. ISAW gồm nhận thức về các chính sách và thủ tục và nhận thức về vai trò và trách nhiệm của mỗi nhân viên trong tổ chức. ISCO được thể hiện qua năng lực của nhân viên, các đánh giá kỹ năng IS, và việc hoàn thành đào tạo và đánh giá nhân viên. ISB được thể hiện qua các cấu trúc gồm sự tuân thủ các chính sách, thủ tục IS và bảo mật thông tin của nhân viên. BI gồm 3 biến quan sát được kế thừa từ Venkatesh and Bala (2008).

3.2. Mẫu nghiên cứu

Dữ liệu được thu thập trực tuyến từ các đối tượng là các nhà quản trị, kế toán viên, kiểm toán viên, nhân viên CNTT/IS là các đối tượng thực hiện công việc liên quan đến IS kế toán. Phương pháp chọn mẫu phi xác suất và thuận tiện được lựa chọn áp dụng với số lượng mẫu là 181. Bảng 1 cho thấy mẫu nghiên cứu có sự đa dạng đặc điểm nhân chủng học của người tham gia khảo sát, do đó, các dữ liệu thu thập là phù hợp cho mục tiêu nghiên cứu.

Bảng 1.
Thống kê mô tả mẫu nghiên cứu

	Số lượng	Tỷ lệ (%)
Lĩnh vực hoạt động		
Sản xuất; sản xuất – thương mại; sản xuất – thương mại - dịch vụ	56	30,9%
Thương mại, Dịch vụ	95	52,5%
Xây dựng	11	6,1%
Khác	19	10,5%
Vị trí công tác		
Trưởng/Phó đơn vị	21	11,6%
Kế toán trưởng	32	17,7%
Kế toán viên/ kiểm soát viên/ kiểm toán viên	83	45,9%
Quản lý các bộ phận	23	12,7%
Nhân viên công nghệ thông tin/ an toàn thông tin	22	12,1%
Kinh nghiệm về IS		
<2 năm	41	22,6%
2–5 năm	72	39,8%
5–10 năm	44	24,3%
>10 năm	24	13,3%
Số năm công tác		
<2 năm	37	20,4%
2–5 năm	63	34,8%
5– 10 năm	41	22,7%
>10 năm	40	22,1%
Tổng	181	100,0%

Một số phân tích được bổ sung để làm tăng độ tin cậy của dữ liệu như đánh giá hiện tượng chệch do không phản hồi và tính vững chắc của dữ liệu (Armstrong & Overton, 1977). Phần mềm SmartPLS được sử dụng và quy trình phân tích được thực hiện theo đề xuất của Hair và cộng sự (2016). Đầu tiên, kiểm định mô hình đo lường để đánh giá giá trị của thang đo, sau đó là kiểm định mô hình cấu trúc để xác định mối quan hệ giữa các cấu trúc. Bên cạnh đó, phân tích post-hoc nhằm bổ sung độ tin cậy và giá trị của nghiên cứu cũng được thực hiện nhằm làm gia tăng giá trị của kết quả nghiên cứu.

4. Kết quả nghiên cứu

4.1. Đánh giá hiện tượng chệch do không phản hồi (Nonresponse Bias Test – NBT) và tính vững chắc của dữ liệu

Kiểm tra NBT có thể xảy ra thông qua thử nghiệm *t*-test. Các câu trả lời khảo sát được chia thành 2 phần gồm những người trả lời sớm và muộn và sự khác biệt trong các biến số nghiên cứu và nhân khẩu học (Armstrong & Overton, 1977). Kết quả phân tích cho thấy không có sự khác biệt trung bình có ý nghĩa thống kê giữa các nhóm; do đó, việc không phản hồi không làm sai lệch kết quả của nghiên cứu.

Giá trị Variance Inflation Factor – VIF được sử dụng để kiểm tra sai lệch do phương pháp (Common Method Variance – CMV) trong phân tích PLS (Kock, 2015). Tất cả các chỉ số VIF đều thấp hơn ngưỡng chấp nhận là 3,3; do đó, CMV không tồn tại. Kỹ thuật FIMIX-PLS được vận dụng để kiểm tra tính không đồng nhất không quan sát được của mẫu nghiên cứu (Hair và cộng sự, 2017). Phân tích FIMIX-PLS dừng lại ở phân khúc thứ 2 do R^2 của phân khúc thứ 3 quá nhỏ ($R^2 = 0,092$) thấp hơn ngưỡng của phân khúc hợp lý là 25%. Các tiêu chí đều cao nhất ở phân khúc thứ 1 so với phân khúc thứ 2. Những kết quả này đã chỉ ra tính không đồng nhất không quan sát không xuất hiện trong dữ liệu nghiên cứu.

4.2. Đánh giá mô hình đo lường

Giá trị của các biến quan sát được đánh giá qua độ tin cậy nhất quán nội tại, giá trị hội tụ, và giá trị phân biệt. Kết quả phân tích lần thứ nhất đã loại 2 biến bao gồm: (1) lo lắng khi báo cáo một cuộc tấn công mạng cho cơ quan thực thi pháp luật vì điều đó có thể gây tổn hại đến danh tiếng của tổ chức, thuộc khái niệm ISA, và (2) hành vi bảo mật, thuộc khái niệm ISB; do hệ số tải thấp hơn 0,7 (Hair và cộng sự, 2016). Sau khi loại 2 biến này, các biến quan sát còn lại đều đảm bảo yêu cầu. Bảng 2 cho thấy tất cả các cấu trúc đều có hệ số Cronbach's Alpha (CA) trên ngưỡng 0,6 và độ tin cậy tổng hợp (Composite Reliability – CR) cao hơn 0,7. Kết quả khẳng định tính nhất quán nội tại của các thang đo cao. Phương sai trung bình được trích xuất (Average Variance Extracted – AVE) của mỗi cấu trúc đều vượt 0,5 (Fornell & Larcker, 1981); và hệ số tải của các cấu trúc đều lớn hơn 0,7 vì vậy giá trị hội tụ của các cấu trúc là đạt được. Giá trị phân biệt của các thang đo đạt được khi Heterotrait-Monotrait Ratio (HTMT) nhỏ hơn 1; do đó, thang đo trong nghiên cứu này đã đạt giá trị phân biệt (Henseler và cộng sự, 2016).

Bảng 2.

Kết quả đánh giá mô hình đo lường

Cấu trúc	Trung bình	Độ lệch chuẩn	Hệ số tải	CA	CR	AVE	VIF
BI	5,643	1,336	(0,879; 0,936)	0,894	0,934	0,825	2,229
ISA	5,208	1,574	(0,859; 1,000)	0,637	0,757	0,354	1,586
ISAW	5,321	1,345	(0,853; 0,897)	0,796	0,799	0,621	1,977
ISB	5,110	1,665	(0,878; 0,918)	0,763	0,781	0,807	–
ISCO	5,140	1,459	(0,912; 1,000)	0,855	0,858	0,776	1,939

4.3. Đánh giá mô hình cấu trúc

Kỹ thuật bootstrapping với 5.000 mẫu lặp lại được sử dụng để ước tính độ lớn và tầm quan trọng của các hệ số đường dẫn (β) ở mức độ tin cậy 95%. Kết quả ở Bảng 3 cho thấy BI bị tác động đáng kể bởi ISAW và ISCO với $p < 0,05$. Trong đó, ISCO tác động đến BI mạnh hơn so với ISAW với hệ số đường dẫn lần lượt là 0,376 và 0,329. Kết quả này xác nhận giả thuyết H_1 và H_3 được chấp nhận. Tuy nhiên, ISA không tác động đến BI với $p = 0,548$; do đó, giả thuyết H_2 bị từ chối. Với sự tác động của biến ngoại sinh, hệ số biến thiên của BI đạt được ở mức tương đối cao (R^2 là 46%).

Sự biến thiên của ISB được xác định bởi các biến trong mô hình nghiên cứu ở mức khá với R^2 là 39,7%. ISB bị ảnh hưởng mạnh nhất bởi BI với $\beta = 0,384$ và $p = 0,000$. ISCO cũng được xác nhận tác động đến ISB nhưng ở mức thấp hơn với $\beta = 0,276$ và $p = 0,008$; khẳng định giả thuyết H_4 và H_6 được chấp nhận. Tuy nhiên, sự tác động của ISA đến ISB bị loại bỏ (giả thuyết H_5) với $p = 0,340$. Hai biến kiểm soát gồm lĩnh vực hoạt động và quy mô hoạt động của đơn vị cũng bị loại bỏ với $p > 0,05$.

Kết quả phân tích vai trò điều tiết của kinh nghiệm bằng phương pháp hai bước (Hair và cộng sự, 2017) cho thấy kinh nghiệm đóng vai trò là biến điều tiết trong mối quan hệ giữa BI và ISB với $p = 0,047$ (giả thuyết H_7 được chấp nhận). Với $\beta = 0,131$ cho thấy kinh nghiệm tác động lên mối quan hệ giữa BI và ISB ở mức độ trung bình. Mức tác động đơn lẻ của BI đến ISB là 0,384 và khi có tác động của biến điều tiết làm cho sự tác động của BI đến ISB tăng lên đạt 0,515.

Bảng 3.

Kết quả đánh giá mô hình cấu trúc

Giả thuyết		R^2	Q^2	f^2	Hệ số đường dẫn (β)	p-value	Kết luận
	BI	0,460	0,364				
H_1	ISAW ➔ BI			0,102	0,329	0,001*	Chấp nhận
H_2	ISA ➔ BI			0,005	0,068	0,548	Bác bỏ
H_3	ISCO ➔ BI			0,153	0,376	0,002*	Chấp nhận
	ISB	0,397	0,286				
H_4	BI ➔ ISB			0,109	0,384	0,000*	Chấp nhận
H_5	ISA ➔ ISB			0,006	0,078	0,340	Bác bỏ
H_6	ISCO ➔ ISB			0,065	0,276	0,008*	Chấp nhận
H_7	Kinh nghiệm ➔ ISB			0,017	0,131	0,047	Chấp nhận
	Lĩnh vực hoạt động ➔ ISB			0,005	–0,054	0,309	Bác bỏ
	Quy mô hoạt động ➔ ISB			0,019	–0,113	0,140	Bác bỏ

Ghi chú: * mức ý nghĩa thống kê 1%

4.4. Phân tích vai trò trung gian

Kết quả phân tích ở Bảng 4 cho thấy ISA không tác động trực tiếp và gián tiếp đến ISB với p > 0,05; do đó, BI không đóng vai trò là trung gian trong mối quan hệ giữa ISA và ISB. ISCO tác động trực tiếp đến ISB và tác động gián tiếp đến ISB thông qua BI. Kết quả khẳng định BI là biến trung gian bổ sung trong mối quan hệ giữa ISCO và ISB.

Bảng 4.

Kết quả phân tích biến trung gian

	Tác động trực tiếp			Tác động gián tiếp		
	Hệ số đường dẫn (β)	p-value	Mức ý nghĩa (Sig.)	Hệ số đường dẫn (β)	p-value	Mức ý nghĩa (Sig.)
ISA ➔ BI ➔ ISB	0,078	0,340	Không	0,026	0,590	Không
ISCO ➔ BI ➔ ISB	0,276	0,008	Có	0,144	0,038	Có

4.5. Phân tích post – hoc

Theo kết quả ở Bảng 3, Q^2 của BI và ISB lớn hơn ngưỡng loại trừ là 0, do đó, có thể kết luận BI và ISB được dự đoán ở mức độ cao trong mô hình. Giá trị f^2 được vận dụng để đánh giá ảnh hưởng của quy mô của từng cấu trúc riêng lẻ với giá trị ngưỡng 0,02; 0,15; và 0,35 tương ứng mức độ tác động lần lượt nhỏ, trung bình và lớn (Hair và cộng sự, 2016). ISCO và ISAW có f^2 ở mức trung bình cho thấy chúng có tác động đến BI. Tuy nhiên, f^2 của ISA rất nhỏ chứng tỏ ISA hầu như không tác động đến BI. Đối với ISB, f^2 của BI ở mức độ trung bình và ISCO ở mức thấp khẳng định 2 biến này có tác động đến ISB. Các biến ISA, lĩnh vực hoạt động, và quy mô hoạt động có f^2 không đáng kể, vì vậy, các biến này hầu như không tác động đến ISB. Kinh nghiệm cũng tác động ở mức tương đối thấp. Bảng 2 cho thấy VIF của các biến độc lập thấp hơn ngưỡng loại trừ là 5. Số liệu này cho thấy hiện tượng đa cộng tuyến không tồn tại giữa các biến độc lập (Hair và cộng sự, 2016).

5. Thảo luận

Kết quả phân tích PLS cho thấy năng lực IS và ISAW ảnh hưởng đáng kể đến BI trong AIS. Cùng với nhau, chúng tạo nên ISC hiệu quả cho doanh nghiệp. Kết quả này phù hợp với các lý thuyết gồm KAB, TRA và TAM. Wang và cộng sự (2022) cũng khẳng định việc đánh giá ISA của người dùng là điều cần thiết để bảo vệ các hệ thống kiểm soát công khỏi các cuộc tấn công kỹ thuật mang tính xã hội, với đối tượng mục tiêu là người sử dụng hệ thống. Những khám phá này cũng xác nhận các kết quả tương tự trong các nghiên cứu trước (Parsons và cộng sự, 2014; Cichowicz và cộng sự, 2021).

Trong bối cảnh Việt Nam, nghiên cứu đã cung cấp các bằng chứng thực nghiệm về tác động của nhận thức, năng lực IS đến ISB trong AIS, khẳng định ISC thực sự là một nguồn lực khan hiếm của tổ chức, phù hợp với RBV. Kết quả này là phù hợp với kết luận của Sulaiman và cộng sự (2022). Parsons và cộng sự (2014) đã cung cấp các bằng chứng để xác nhận nếu nhân viên tuân theo các quy tắc và quy định an toàn, nó sẽ giúp tăng cường IS. Ngoài ra, Warkentin và cộng sự (2016) kết luận

ISC là một thành phần đa hướng có vai trò quan trọng trong ngăn chặn và phát hiện các hành vi gây mất IS hay nguy hại cho hệ thống thông tin của tổ chức. Chúng tôi cũng tìm thấy sự tương đồng trong kết quả nghiên cứu này với Gioulekas và cộng sự (2022).

Khám phá thú vị của nghiên cứu này là đã chứng minh vai trò điều tiết của kinh nghiệm của nhân viên cho tác động của BI đến ISB. Các nghiên cứu trước (Hwang và cộng sự, 2019; Khando và cộng sự, 2021) đã chứng minh tác động của kinh nghiệm đến ISB.

Trái với các giả thuyết ban đầu, những phân tích PLS cho thấy thái độ không ảnh hưởng trực tiếp đến BI và ISB. Kết quả này không tương đồng với khám phá của Townsend III (2022). Tuy nhiên, Sas và cộng sự (2021) đã kết luận tương tự không chứng thực về tác động của thái độ đối với ISB.

6. Kết luận và hàm ý quản trị

6.1. Kết luận

Trong bối cảnh nguy cơ về IS, đặc biệt thông tin kế toán ngày càng trở thành mối quan tâm của các doanh nghiệp, nghiên cứu này quan tâm đến các khía cạnh của ISC và mối quan hệ của chúng trong AIS. Kết quả cho thấy các yếu tố của ISC có quan hệ mật thiết với nhau. ISAW và năng lực IS của nhân viên là hai cấu trúc ảnh hưởng mạnh đến BI trong AIS. Nghiên cứu này cũng xác nhận tầm quan trọng của các cấu trúc trong ISC đối với ISB. Cuối cùng, các bằng chứng thực nghiệm đã chứng minh tác động điều tiết của kinh nghiệm đối với tác động của BI đến ISB. Từ các kết quả nghiên cứu, chúng tôi đã phát triển những hàm ý quản trị đối với các nhà quản trị nhằm đạt được các mục tiêu IS kế toán. Nghiên cứu này cũng tồn tại một số hạn chế bao gồm:

- *Thứ nhất*, do phạm vi của nghiên cứu chỉ tập trung vào tác động của các cấu trúc trong ISC, do đó, khả năng giải thích cho ISB đang đạt ở mức độ trung bình. Các nghiên cứu sau nên bổ sung các cấu trúc có ảnh hưởng đến ISB.

- *Thứ hai*, mẫu nghiên cứu mặc dù khá đa dạng và cỡ mẫu cũng đảm bảo yêu cầu phân tích dữ liệu theo PLS; tuy nhiên, để tăng khả năng đại diện cho tổng thể, các nhà nghiên cứu nên mở rộng cỡ mẫu cũng như các đối tượng khảo sát. Các nghiên cứu tương lai có thể mở rộng phạm vi nghiên cứu trên các hệ thống thông tin con khác.

6.2. Hàm ý quản trị

Kết quả nghiên cứu hỗ trợ nhà quản trị hiểu biết rõ hơn về ISC và mối quan hệ giữa các yếu tố của nó trong AIS, từ đó, xây dựng các chiến lược phát triển và thay đổi ISC. Để cải thiện ISB, nhà quản trị cần chú trọng nâng cao nhận thức và năng lực về IS các nhân viên. Hiện tại, nhận thức, năng lực và BI của các nhân viên tại các doanh nghiệp Việt Nam chỉ ở mức trung bình khá với mức đánh giá 5/7 điểm. Do đó, các doanh nghiệp cần cải thiện các yếu tố này nhằm gia tăng ISB. Các nhà quản lý cũng cần chú trọng xây dựng ISC cụ thể, thống nhất và truyền thông rõ ràng các chính sách, và ISC đến toàn thể nhân viên để họ có thể hiểu biết và nhận thức được chính xác các chiến lược phát triển ISC của doanh nghiệp; và từ đó thực hiện đúng chiến lược. Doanh nghiệp cũng cần làm cho nhân viên nhận thức rõ được trách nhiệm và vai trò của mình về các hoạt động liên quan đến IS. Kinh nghiệm về ISC đóng vai trò điều tiết trong mối quan hệ giữa BI và ISB, do đó, các nhà quản lý nên chú trọng

vào công tác đào tạo, huấn luyện về IS để nâng cao trình độ, kinh nghiệm của nhân viên về IS kế toán giúp giảm thiểu các lỗi sai và các rủi ro liên quan đến IS.

Lời cảm ơn

Nghiên cứu này được tài trợ bởi Đại học Kinh tế Thành phố Hồ Chí Minh trong khuôn khổ của đề tài nghiên cứu khoa học số CS-COB-2022-20.

Tài liệu tham khảo

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211.

Al-Fatlawi, Q. A., Al Farttoosi, D. S., & Almagtome, A. H. (2021). Accounting information security and it governance under cobit 5 framework: A case study. *Webology*, *18*(Special Issue on Information Retrieval and Web Search), 294–310.

Alfawaz, S., Nelson, K., & Mohannak, K. (2010, January). Information security culture: a behaviour compliance conceptual framework. In *Proceedings of the 8th Australasian Information Security Conference* (AISC 2010) (Vol. 105, pp. 47–55). University of Southern Queensland.

Alhogail, A., & Mirza, A. (2014). A framework of information security culture change. *Journal of Theoretical & Applied Information Technology*, *64*(2), 540–549.

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences*, *11*(8), 3383. doi: 10.3390/app11083383

Almagtome, A., Khaghaany, M., & Önce, S. (2020). Corporate governance quality, stakeholders' pressure, and sustainable development: An integrated approach. *International Journal of Mathematical Engineering and Management Sciences*, *5*(6), 1077–1090.

Armstrong, J. S., & Overton, T. S. (1977). Estimating nonresponse bias in mail surveys. *Journal of Marketing Research*, *14*(3), 396–402.

Bawaneh, S. S. (2014). Information security for organizations and accounting information systems a Jordan banking sector case. *International Review of Management and Business Research*, *3*(2), 1174–1188.

Cichowicz, E., Iwanicz-Drozdowska, M., & Kurowski, Ł. (2021). “Every knock is a boost”. Cyber risk behaviour among Poles. *Economics and Business Review*, *7*(4), 94–120.

da Veiga, A. (2018). An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture. *Information & Computer Security*, 26(5), 584–612.

da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture - Perspectives from academia and industry. *Computers & Security*, *92*, 101713.

Dandago, K. I., & Rufai, A. S. (2014). Information technology and accounting information system in the Nigerian banking industry. *Asian Economic and Financial Review*, *4*(5), 655–670.

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*, *22*(5), 474–489.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 319–340.

Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research.* Reading, MA: Addison-Wesley.

Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of Marketing Research*, *18*, 382–388.

Furnell, S., & Rajendran, A. (2012). Understanding the influences on information security behaviour. *Computer Fraud & security*, *2012*(3), 12–15.

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Designing a cyber-security culture assessment survey targeting critical infrastructures during COVID-19 crisis. *International Journal of Network Security & Its Applications*, *13*(1), 33–50.

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2020). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems*, *62*(3), 452–462.

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., ... & Baker, T. (2018). Security threats to critical infrastructure: The human factor. *The Journal of Supercomputing*, *74*, 4986–5002.

Sánchez-Caballé, A., Gisbert, C. M., & Esteve-Mon, F. M. (2020). The digital competence of university students: A systematic literature review. *Aloma, 38*(1), 63–74.

Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Georgiadou, A., Michalitsi-Psarrou, A., ... & Ntanos, C. (2022). A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures. *Healthcare*, *10*(2), 327. doi: 10.3390/healthcare10020327

Hadlington, L., & Murphy, K. (2018). Is media multitasking good for cybersecurity? Exploring the relationship between media multitasking and everyday cognitive failures on self-reported risky cybersecurity behaviors. *Cyberpsychology, Behavior, and Social Networking*, *21*(3), 168–172.

Haeussinger, F., & Kranz, J. (2013). Information security awareness: Its antecedents and mediating effects on security compliant behavior. In *Proceedings of the 34th International Conference on Information Systems (ICIS 2013)*. Milan, Italy.

Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Sage Publications.

Hair Jr, J. F., Sarstedt, M., Ringle, C. M., & Gudergan, S. P. (2017). *Advanced issues in partial least squares structural equation modeling*. Sage Publications.

Henseler, J., Hubona, G., & Ray, P. A. (2016). Using PLS path modeling in new technology research: Updated guidelines. *Industrial Management & Data Systems*, *116*(1), 2–20.

Humaidi, N., & Balakrishnan, V. (2015). The moderating effect of working experience on health information system security policies compliance behaviour. *Malaysian Journal of Computer Science*, *28*(2), 70–92.

Huzaizi, A. H. A., Tajuddin, S. N. A. A., Bahari, K. A., Manan, K. A., & Mubin, N. N. A. (2021). Cyber-security culture towards digital marketing communications among small and medium-sized (SME) entrepreneurs. *Asian Culture and History*, *13*(2), 1–20.

Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2019). Security awareness: The first step in information security compliance behavior. *Journal of Computer Information Systems*, *61*(4), 345–356.

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, *106*, 102267.

Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of e-Collaboration*, *11*(4), 1–10.

Marks, A. (2007). *Exploring universities' information systems security awareness in a changing higher education environment: a comparative case study research*. PhD thesis, University of Salford.

McFarland, D. J., & Hamilton, D. (2006). Adding contextual specificity to the technology acceptance model. *Computers in Human Behavior*, *22*(3), 427–447.

Ngo, L., Zhou, W., & Warren, M. (2005). Understanding transition towards information security culture change. *Proceeding of the 3rd Australian Computer, Network & Information Forensics [42] Conference, Edith Cowan University, School of Computer and Information Science*, 67–73.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security*, *42*, 165–176.

Peteraf, M. A. (1993). The cornerstones of competitive advantage: A resource-based view. *Strategic Management Journal*, *14*(3), 179–191.

Ponemon. (2018). *Cost of data breach study: Impact of business continuity management.* Retrieved from https://whitepapers.theregister.com/paper/view/7188/cost-of-data-breach-study-impact-of-business-continuity-management

Poon, W. C. (2008). Users' adoption of e-banking services: The Malaysian perspective. *Journal of Business & Industrial Marketing*, *23*(1), 59–69.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, *27*(7–8), 241–253.

Ricci, J., Breitinger, F., & Baggili, I. (2019). Survey results on adults and cybersecurity education. *Education and Information Technologies*, *24*, 231–249.

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security*, *26*(1), 56–62.

Sas, M., Reniers, G., Ponnet, K., & Hardyns, W. (2021). The impact of training sessions on physical security awareness: Measuring employees' knowledge, attitude and self-reported behaviour. *Safety Science*, *144*, 105447.

Schrader, P. G., & Lawless, K. A. (2004). The knowledge, attitudes, & behaviors approach how to evaluate performance and learning in complex environments. *Performance Improvement*, *43*(9), 8–15.

Simkin, M. G., Norman, C. A. S., & Rose, J. M. (2014). *Core Concepts of Accounting Information Systems*. John Wiley & Sons.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31–41.

Sulaiman, N. S., Fauzi, M. A., Wider, W., Rajadurai, J., Hussain, S., & Harun, S. A. (2022). Cyber–Information security compliance and violation behaviour in organisations: A systematic review. *Social Sciences*, *11*(9), 386.

Taiwo, J. N. (2016). Effect of ICT on accounting information system and organisational performance: The application of information and communication technology on accounting information system. *European Journal of Business and Social Sciences*, *5*(2), 1–15.

Townsend III, H. E. (2022). *An examination of the significance of security knowledge and attitudes on security behavior* [Doctoral dissertation, Capella University].

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109*, 102387.

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*, *39*(2), 273–315.

Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, *23*(3), 191–198.

Wang, K., Guo, X., & Yang, D. (2022). Research on the effectiveness of cyber security awareness in ICS risk assessment frameworks. *Electronics*, *11*(10), 1659. doi: 10.3390/electronics11101659

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems*, *92*, 25–35.

Westera, W. (2001). Competences in education: A confusion of tongues. *Journal of Curriculum Studies*, *33*(1), 75–88.

Whitman, M. E., & Mattord, H. J. (2016). *Management of information security*. Cengage Learning.

Yaokumah, W., Walker, D. O., & Kumah, P. (2019). SETA and security behavior: Mediating role of employee relations, monitoring, and accountability. *Journal of Global Information Management*, *27*(2), 102–121.

Zakaria, O., Gani, A., Nor, M. M., & Anuar, N. B. (2007). *Reengineering information security culture formulation through management perspective*. International Conference on Electrical Engineering and Informatics, Indonesia. Retrieved from https://www.academia.edu/2612533/Reengineering_Information_Security_Culture_Formulation_Through_Management_Perspective