Tạp chí Nghiên cứu Kinh tế và Kinh doanh Châu Á
Năm thứ 36, Số 7 (2025), 22-37

www.jabes.ueh.edu.vn

JABES

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

Nâng cao thành quả an toàn thông tin: Vai trò của hành vi né tránh nguy cơ và sự sẵn sàng của doanh nghiệp

NGUYỄN HỮU BÌNH [*,a], PHẠM TRÀ LAM [a], NGUYỄN PHƯỚC BẢO ẤN [a], NGUYỄN QUỐC TRUNG [a]

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

THÔNG TIN

Ngày nhận: 25/06/2025
Ngày nhận lại: 27/08/2025
Duyệt đăng: 30/08/2025

Mã phân loại JEL:
M12; M15.

Từ khóa:
Thành quả an toàn thông tin;
Sự sẵn sàng đối với an toàn thông tin;
Hành vi né tránh nguy cơ;
Việt Nam.

Keywords:
Information security performance;
Information security readiness;

TÓM TẮT

Các nguy cơ đối với an toàn thông tin (Information Security – ISe) ngày càng nhiều và tác động nghiêm trọng đến hoạt động kinh doanh bền vững, nhưng không có nhiều nghiên cứu về thành quả ISe từ góc nhìn quản trị con người. Vì vậy, nghiên cứu này được thực hiện để kiểm tra mô hình nhằm giải thích cách thức thành quả ISe bị ảnh hưởng bởi sự sẵn sàng đối với ISe, hành vi né tránh nguy cơ, và các yếu tố khác. Kết quả phân tích bình phương nhỏ nhất từng phần (Partial Least Squares – PLS) dữ liệu của 320 doanh nghiệp cho thấy sự sẵn sàng đối với ISe là trung gian toàn phần cho tác động của hành vi né tránh nguy cơ đến thành quả ISe. Nghiên cứu cũng xác nhận vai trò quan trọng của động lực né tránh nguy cơ, chương trình giáo dục, huấn luyện, và nâng cao nhận thức về ISe, và ảnh hưởng xã hội đến cả hành vi né tránh nguy cơ và sự sẵn sàng đối với ISe. Các khám phá này đã hỗ trợ nhà quản trị doanh nghiệp, công ty tư vấn về ISe, và các cơ quan nhà nước có thẩm quyền những hiểu biết về chiến lược tăng cường thành quả ISe.

Abstract

Information security (ISe) threats are increasing and seriously impacting sustainable business operations. Due to the lack of studies on ISe performance from a human resource management perspective, this study tested a model to explain how ISe performance is affected by ISe readiness, threat avoidance behavior, and other antecedents.

[*] Tác giả liên hệ.
Biên tập viên: Nguyễn Lương Tâm.
Email: huubinh_ais@ueh.edu.vn (Nguyễn Hữu Bình); phamtralamais@ueh.edu.vn (Phạm Trà Lam); baoan@ueh.edu.vn (Nguyễn Phước Bảo Ấn); nguyenquoctrung@ueh.edu.vn (Nguyễn Quốc Trung).
Trích dẫn bài viết: Nguyễn Hữu Bình, Phạm Trà Lam, Nguyễn Phước Bảo Ấn, & Nguyễn Quốc Trung. (2025). Nâng cao thành quả an toàn thông tin: Vai trò của hành vi né tránh nguy cơ và sự sẵn sàng của doanh nghiệp. *Tạp chí Nghiên cứu Kinh tế và Kinh doanh Châu Á, 36*(7), 22-37. https://doi.org/10.24311/jabes/2025.36.7.02

Threat avoidance behavior; Vietnam.	The PLS analysis of 320 enterprises showed that ISe readiness fully mediated the impact of threat avoidance behavior on ISe performance. The authors also confirmed the significant roles of risk avoidance motivation, ISe education, training, awareness programs, and social influence on threat avoidance behavior and ISe readiness. These findings provide business managers, ISe consulting firms, and authorities with insights into strategies to enhance ISe performance.

1. Giới thiệu

Trong thời đại số ngày nay, các tổ chức ngày càng phụ thuộc vào hệ thống thông tin (Information Systems – IS) để gia tăng hiệu quả hoạt động kinh doanh và duy trì lợi thế chiến lược. Tuy nhiên, sự phụ thuộc này cũng mang đến những rủi ro đáng kể, đặc biệt trong bối cảnh các hình thức tấn công mạng và vi phạm ISe đang leo thang trên toàn thế giới (Khando và cộng sự, 2021). Báo cáo tình hình an ninh mạng Việt Nam 2024 ghi nhận số lượng kỷ lục các loại mã độc, các chiến dịch tấn công có chủ đích, biến thể ứng dụng ngân hàng di động Trojan tấn công hơn 50 ứng dụng tài chính và ví điện tử tại Việt Nam, các hoạt động đánh cắp thông tin trình duyệt, thông tin nhạy cảm của tổ chức,… đã tấn công thành công vào nhiều cơ quan chính phủ, doanh nghiệp và các tổ chức tài chính ở nước ta (NCSGroup, 2025). Tại Việt Nam, năm 2023 đã xảy ra 13.900 cuộc tấn công mạng, trung bình 1.160 vụ/tháng, gây thiệt hại hơn 390.000 tỷ đồng (tương đương 3,6% GDP). NCS (2024) dự báo năm 2025 sẽ là năm của các cuộc tấn công vào hệ thống đám mây và các chuỗi cung ứng, hay các tấn công API.

Thống kê trên cho thấy các doanh nghiệp đang phải đối mặt với nhiều mối đe dọa đối với ISe. Khi các mối đe dọa gia tăng, các tổ chức buộc phải ưu tiên các giải pháp gia tăng thành quả ISe (Organization Security Performance – OSP) để bảo vệ dữ liệu nhạy cảm, duy trì tính liên tục của hoạt động và bảo vệ danh tiếng của họ (Whitman & Mattord, 2022). Mặc dù vấn đề này ngày càng cấp bách, phần lớn các nghiên cứu hiện đang tập trung vào các khía cạnh kỹ thuật của ISe, thường bỏ qua các yếu tố quan trọng liên quan đến con người và tổ chức.

Các nghiên cứu trước chủ yếu tập trung vào OSP ở các nước phát triển, trong khi chủ đề này ở các nước đang phát triển còn khan hiếm. Các quốc gia này phải đối mặt với nhiều thách thức, bao gồm nguồn lực, kiến thức hạn chế, và môi trường văn hóa xã hội phức tạp, có thể cản trở tiến trình thúc đẩy OSP (Rezgui & Marks, 2008). Nghiên cứu về OSP vẫn còn trong giai đoạn sơ khai tại Việt Nam. Do đó, nghiên cứu này xem xét các yếu tố ảnh hưởng đến OSP, tập trung vào hành vi né tránh nguy cơ (Liang & Xue, 2009) và sự sẵn sàng đối với ISe (Security Readiness – CSR) (Rîndaşu, 2017).

Tổng quan nghiên cứu cho thấy có nhiều nhân tố ảnh hưởng đến OSP. Trong nghiên cứu này, nhóm tác giả khám phá cách các đặc điểm cá nhân của nhân viên bao gồm động lực né tránh nguy cơ (Young và cộng sự, 2016), niềm tin đạo đức của nhân viên (Lankton và cộng sự, 2019) và các yếu tố môi trường gồm ảnh hưởng của xã hội (Samtani và cộng sự, 2019), quy tắc đạo đức (Nemati, 2007) và chương trình giáo dục, huấn luyện và nâng cao nhận thức về ISe (Security Education Training Awareness – SETA) (Burns và cộng sự, 2018) tác động đến sự sẵn sàng và hành vi né tránh nguy cơ ISe. Mặc dù, các nghiên cứu trước đã khám phá rời rạc về mối quan hệ giữa các yếu tố này, chưa có sự tích hợp hai nhóm nhân tố liên quan đến đặc điểm tính cách và môi trường bên ngoài trong nghiên

cứu ISe. Những phát hiện từ nghiên cứu này cung cấp các bằng chứng thực nghiệm để các nhà quản trị xây dựng chiến lược nhằm tăng cường OSP.

2. Cơ sở lý thuyết

ISe là bảo vệ thông tin và các yếu tố quan trọng của nó, bao gồm các hệ thống và phần cứng dùng để sử dụng, lưu trữ và truyền tải thông tin (Whitman & Mattord, 2022). Trong bối cảnh các nguy cơ ISe ngày càng gia tăng, OPS trở thành yếu tố được các tổ chức đặc biệt quan tâm. Theo Hasan và cộng sự (2021), OPS là lợi ích mà tổ chức mong đợi từ các biện pháp bảo vệ thông tin, thể hiện qua khả năng đảm bảo tính bảo mật, toàn vẹn, và khả dụng của tài sản thông tin.

Trong ISe, việc đối phó hữu hiệu với các nguy cơ phụ thuộc rất nhiều vào những hành vi phù hợp từ phía người dùng cuối (Whitman & Mattord, 2022). Do vậy, hiểu biết sâu sắc về hành vi né tránh nguy cơ của người dùng là điều cần thiết để đảm bảo ISe (Liang & Xue, 2009). Theo DeLone và McLean (2003), hành vi sử dụng IS tác động mạnh mẽ đến các lợi ích thu được từ hệ thống. Theo đó, khi người dùng chủ động thực hiện những hành vi sử dụng hệ thống theo hướng đảm bảo an toàn, như sử dụng mật khẩu mạnh, tránh nhấp vào liên kết đáng ngờ sẽ giúp giảm thiểu rủi ro từ các nguy cơ, từ đó nâng cao OSP. Do đó, nhóm tác giả phát triển giả thuyết H_1 như sau:

Giả thuyết H_1: Hành vi né tránh nguy cơ ảnh hưởng tích cực đến OSP.

CSR là mức độ nhận thức, sự chuẩn bị và cam kết của một tổ chức trong việc bảo vệ tài sản thông tin khỏi các nguy cơ (Hasan và cộng sự, 2021). Sự phát triển của công nghệ, tấn công mạng ngày càng tinh vi và thường xuyên đã làm gia tăng lo ngại về ISe. Nếu thiếu đi CSR, các tổ chức sẽ gặp nhiều khó khăn trong việc thiết lập mức độ ISe phù hợp (Rîndaşu, 2017)**.** Khi các tổ chức tăng cường sự sẵn sàng về an ninh mạng, họ sẽ đạt được thành quả an toàn vượt trội bằng cách giảm vi phạm dữ liệu theo thời gian, có được danh tiếng bảo mật hợp pháp, tăng cường tính an toàn của các quy trình nội bộ và phát triển một hệ thống đáng tin cậy (Hasan và cộng sự, 2021). Từ các bằng chứng trên, nhóm tác giả xây dựng giả thuyết H_2 như sau:

Giả thuyết H_2: CSR ảnh hưởng tích cực đến OSP.

Con người là mắt xích yếu nhất trong ISe (Lebek và cộng sự, 2013),; do đó, dù có áp dụng các kiểm soát công nghệ mạnh mẽ, tổ chức vẫn khó đạt được trạng thái sẵn sàng an toàn nếu nhân viên thiếu động lực và hành vi phù hợp để né tránh nguy cơ. Theo lý thuyết sẵn sàng thay đổi của tổ chức (Organizational Readiness for Change – ORC), sự sẵn sàng ở cấp độ tổ chức phản ánh mức độ chuẩn bị tâm lý và hành vi của các thành viên để thực hiện thay đổi, bao gồm cam kết, và hiệu quả thay đổi (Weiner, 2020). Theo đó, khi nhân viên chủ động thực hiện các hành vi né tránh nguy cơ, họ có thể góp phần vào hai khía cạnh quan trọng của sự sẵn sàng bao gồm cam kết thay đổi – thể hiện quyết tâm chung theo đuổi hành động an toàn, và hiệu quả thay đổi – niềm tin tập thể vào khả năng tổ chức và thực hiện các hành động cần thiết để đảm bảo ISe (Weiner, 2020). Trên cơ sở đó, giả thuyết H_3 sau được thiết lập:

Giả thuyết H_3: Hành vi né tránh nguy cơ ảnh hưởng tích cực đến CSR.

Đặc điểm cá nhân và An toàn thông tin

Động lực được xem là yếu tố quan trọng thúc đẩy hành vi cá nhân. Lý thuyết kỳ vọng cho rằng con người có xu hướng chọn hành vi mang lại phần thưởng cao nhất (Vroom, 1964). Theo lý thuyết

né tránh nguy cơ về công nghệ, người dùng chủ động thực hiện hành vi bảo vệ khi tin vào hiệu quả của giải pháp (Liang & Xue, 2009). Động lực né tránh nguy cơ là yếu tố trung tâm thúc đẩy hành vi phòng ngừa trong lý thuyết động lực bảo vệ (Rogers, 1975, 1983). Người dùng sẽ thực hiện các hành vi né tránh nguy cơ khi họ có động lực để thực hiện, động lực này thường được định hình bởi sự hiểu biết của cá nhân về mối đe dọa và mức độ tự tin của họ trong việc giảm thiểu rủi ro đó (Carpenter và cộng sự, 2019).

Theo lý thuyết ORC (Weiner, 2020), sự sẵn sàng thay đổi của tổ chức thể hiện qua "*quyết tâm chung của các thành viên trong tổ chức để theo đuổi các hành động liên quan đến việc thực hiện thay đổi*". Khi cá nhân có động lực cao để né tránh nguy cơ, họ nhận thức rõ hơn về sự cần thiết và tầm quan trọng của các biện pháp ISe, từ đó gia tăng cam kết thay đổi ở cấp độ tổ chức. Khi nhiều thành viên cùng chia sẻ động lực mạnh mẽ đó, quyết tâm chung sẽ được củng cố, góp phần thúc đẩy mức độ sẵn sàng cao hơn cho việc triển khai các thay đổi về ISe. Do đó, nhóm tác giả phát triển giả thuyết H_{4a} và H_{4b} như sau:

Giả thuyết H_{4a}: Động lực né tránh nguy cơ ảnh hưởng tích cực đến hành vi né tránh nguy cơ.

Giả thuyết H_{4b}: Động lực né tránh nguy cơ ảnh hưởng tích cực đến CSR.

Theo lý thuyết ra quyết định đạo đức (Lincoln & Holmes, 2011), niềm tin đạo đức là mức độ một người cảm nhận một hành vi cụ thể có sai trái về mặt đạo đức (D'Arcy & Devaraj, 2012), đóng vai trò định hướng cá nhân trong việc đánh giá về mặt đạo đức trước khi hành động. Quan điểm này được củng cố bởi lý thuyết lựa chọn hợp lý hiện đại, vốn cho rằng con người có thể kiềm chế hành vi không chỉ vì lo sợ bị trừng phạt, mà còn do nhận thức hành vi đó là sai trái về mặt đạo đức (Vance & Siponen, 2012). Trong môi trường công nghệ, những nhân viên có niềm tin đạo đức mạnh mẽ có xu hướng ít lạm dụng hệ thống hoặc ít vi phạm các chính sách ISe, vì họ coi việc không tuân thủ là vi phạm các tiêu chuẩn đạo đức (Chatterjee và cộng sự, 2015).

Từ lý thuyết ORC (Weiner, 2020), niềm tin mạnh mẽ vào các hành vi đạo đức ISe ở cấp độ cá nhân có thể thúc đẩy cam kết thay đổi đối với ISe ở cấp độ tổ chức. Khi các cá nhân tin rằng việc tuân thủ các hành vi đạo đức ISe là đúng đắn và quan trọng, họ sẽ có xu hướng ủng hộ và cam kết thực hiện các thay đổi nhằm tăng cường ISe. Do đó, nhóm tác giả phát triển giả thuyết H_{5a} và H_{5b} như sau:

Giả thuyết H_{5a}: Niềm tin đạo đức ảnh hưởng tích cực đến hành vi né tránh nguy cơ.

Giả thuyết H_{5b}: Niềm tin đạo đức ảnh hưởng tích cực đến CSR.

Bối cảnh môi trường và An toàn thông tin

Sự thay đổi trong niềm tin, cảm xúc hoặc hành vi cá nhân có thể phát sinh từ quá trình tương tác với môi trường xã hội – hiện tượng này được gọi là ảnh hưởng xã hội (Rashotte, 2007). Trong bối cảnh công nghệ, ảnh hưởng xã hội định hình cách người dùng nhận thức, đánh giá về mức độ nghiêm trọng, tính dễ bị tổn thương, và hiệu quả đối phó với các rủi ro. Theo lý thuyết động lực bảo vệ và lý thuyết né tránh nguy cơ công nghệ, những yếu tố này sẽ thúc đẩy hành vi né tránh nguy cơ ISe. Điều này cũng phù hợp với quan điểm cho rằng các chuẩn mực xã hội sẽ định hướng hành vi phòng ngừa rủi ro của cá nhân trên cơ sở lý thuyết hành vi dự định, lý thuyết thuyết phục bằng nỗi sợ (Johnston & Warkentin, 2010) và các kết quả nghiên cứu thực nghiệm (Samtani và cộng sự, 2019). Những phân tích trên cho thấy ảnh hưởng xã hội giữ vai trò quan trọng trong định hình hành vi cá nhân. Sự khuyến khích hoặc áp lực từ cộng đồng, đồng nghiệp hay cấp trên có thể giảm cảm nhận rủi ro, tăng lòng tin và thúc đẩy tuân thủ các biện pháp ISe, nhất là trong các nền văn hóa tập thể. Mạng xã hội và các

chiến dịch truyền thông ngày càng trở nên hiệu quả trong việc lan tỏa thông tin về rủi ro, nâng cao nhận thức và thúc đẩy hành vi phòng ngừa của người dùng. Do đó, nhóm tác giả đề xuất giả thuyết H_{6a} và H_{6b} như sau:

Giả thuyết H_{6a}: Ảnh hưởng xã hội tác động tích cực đến hành vi né tránh nguy cơ.

Giả thuyết H_{6b}: Ảnh hưởng xã hội tác động tích cực đến CSR.

Quy tắc đạo đức được xem như "vùng trung gian" giữa các giá trị xã hội và luật pháp, trong đó các chế tài xã hội được sử dụng để đảm bảo sự tuân thủ các hành vi chuẩn mực (Molander, 1987). Trong lĩnh vực CNTT, đạo đức và ISe được xem là hai yếu tố song hành, trong đó đạo đức là nền tảng của ISe (Nemati, 2007). Tuy nhiên, sự khác biệt văn hóa khiến việc xác định đâu là hành vi đạo đức trong sử dụng công nghệ trở nên phức tạp (Whitman & Mattord, 2022). Do vậy, nhiều tổ chức nghề nghiệp như ACM, ISC², và ISSA đã ban hành các quy tắc đạo đức để chuẩn hóa và định hướng hành vi trong sử dụng công nghệ và bảo vệ IS. Ở cấp độ tổ chức, các quy tắc đạo đức đóng vai trò quan trọng trong thúc đẩy hành vi ISe và sự sẵn sàng bảo vệ thông tin của nhân viên. Khi cá nhân nhận thức rõ các tiêu chuẩn đạo đức cần tuân thủ, họ có xu hướng né tránh các hành vi gây nguy cơ mất an toàn và chủ động thực hiện các biện pháp phòng ngừa. Từ lập luận này, giả thuyết H_{7a} và H_{7b} được đề xuất như sau:

Giả thuyết H_{7a}: Quy tắc đạo đức tác động tích cực đến hành vi né tránh nguy cơ.

Giả thuyết H_{7b}: Quy tắc đạo đức tác động tích cực đến CSR.

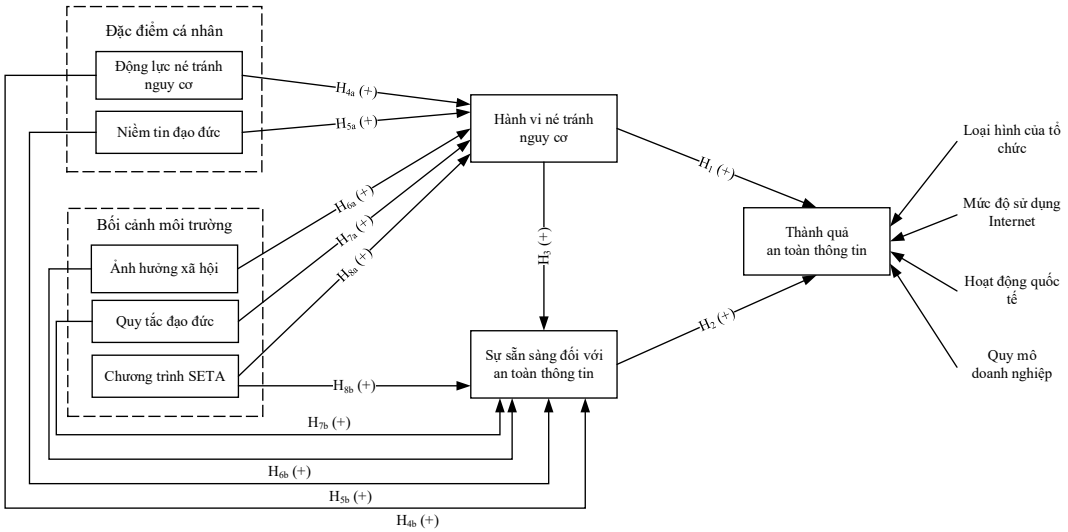
Một tổ chức với các biện pháp phòng vệ kỹ thuật tốt nhất vẫn có thể gặp phải các vấn đề nghiêm trọng về ISe do lỗi của con người, do đó, SETA được xem là giải pháp cần thiết để đảm bảo ISe (Whitman & Mattord, 2022). SETA là những nỗ lực liên tục nhằm thúc đẩy nhận thức của nhân viên về các vấn đề an toàn và cung cấp cho họ kiến thức và kỹ năng để chống lại các rủi ro ISe (Burns và cộng sự, 2018). Theo lý thuyết học tập xã hội (Bandura & Walters, 1977), SETA được cho là có ảnh hưởng đến hành vi né tránh nguy cơ thông qua quá trình học hỏi từ quan sát và trải nghiệm xã hội. Nhân viên học cách ứng xử phù hợp khi nhận thấy phần thưởng cho hành vi đúng và hình phạt cho hành vi sai. SETA hiệu quả giúp tăng ý định tuân thủ chính sách (Burns và cộng sự, 2018), giảm lạm dụng hệ thống (Lee và cộng sự, 2004), và nâng cao trách nhiệm bảo vệ thông tin (Puhakainen & Siponen, 2010). Từ đó, nhóm tác giả phát triển giả thuyết H_{8a} và H_{8b} như sau:

Giả thuyết H_{8a}: SETA tác động tích cực đến hành vi né tránh nguy cơ.

Giả thuyết H_{8b}: SETA tác động tích cực đến CSR.

Biến kiểm soát

Nghiên cứu này xem xét bốn biến kiểm soát gồm loại hình tổ chức, mức độ sử dụng Internet, hoạt động quốc tế, và quy mô doanh nghiệp. Các loại hình doanh nghiệp khác nhau có thể đối mặt với mức độ rủi ro và yêu cầu tuân thủ khác nhau, từ đó ảnh hưởng đến chiến lược ISe (Ernest & Ho, 2006). Mức độ sử dụng Internet cao thường đi kèm với rủi ro an ninh lớn hơn, đặc biệt khi tổ chức phụ thuộc vào nền tảng trực tuyến, IoT hoặc điện toán đám mây, khiến họ có xu hướng áp dụng các biện pháp an toàn nghiêm ngặt hơn (Federal Bureau of, 2023). Hoạt động quốc tế làm gia tăng sự phức tạp trong việc tuân thủ các quy định an toàn khác nhau và đối phó với nguy cơ đa dạng (Meltzer, 2020). Quy mô doanh nghiệp ảnh hưởng đáng kể đến mức độ đầu tư vào ISe. Doanh nghiệp lớn có nhiều nguồn lực để triển khai ISe, trong khi các doanh nghiệp nhỏ thường gặp khó khăn về ngân sách và chuyên môn, dẫn đến khả năng an toàn hạn chế và rủi ro cao hơn (Cisco Systems, 2023).



Hình 1. Mô hình nghiên cứu

3. Phương pháp nghiên cứu

3.1. Đo lường

Thang đo của các cấu trúc được kế thừa từ các nghiên cứu trước và được điều chỉnh phù hợp với bối cảnh ISe. Các biến quan sát được thiết kế dưới dạng câu hỏi theo thang đo Likert 7 điểm, với các mức phản hồi từ 1 (Hoàn toàn không đồng ý) đến 7 (Hoàn toàn đồng ý). OSP và CSR đều được đo lường dựa vào Hasan và cộng sự (2021). OSP là một cấu trúc đơn hướng gồm 5 biến. CSR có dạng kết quả - kết quả với 5 cấu trúc bậc nhất: nhận biết (CSRI: 3 biến), sự bảo vệ (CSRP: 3 biến), phát hiện (CSRD: 3 biến), phản ứng (CSRRs: 3 biến), và phục hồi (CSRRc: 2 biến). Hành vi né tránh nguy cơ (TAB: 2 biến) và động lực né tránh nguy cơ (TAM: 3 biến) được chấp nhận theo Davis và cộng sự (1989). Thang đo của niềm tin đạo đức (MRB: 3 biến) và SETA (5 biến) được kế thừa theo D'Arcy và cộng sự (2009). Ảnh hưởng xã hội (SI) là một cấu trúc gồm 3 biến theo Venkatesh và cộng sự (2012). Quy tắc đạo đức (EC) được đo lường qua 10 biến theo đề xuất của Nemati (2007). Tất cả các cấu trúc đơn hướng đều có dạng thang đo kết quả.

3.2. Mẫu nghiên cứu

Đối tượng thu thập dữ liệu là những cá nhân vận hành và sử dụng IS của doanh nghiệp được lựa chọn theo phương pháp thuận tiện. Mẫu nghiên cứu gồm 320 doanh nghiệp với sự đa dạng theo quy mô, số năm hoạt động của doanh nghiệp, loại hình kinh doanh, và loại hình sở hữu (Bảng 1).

Bảng 1.

Thống kê đặc điểm doanh nghiệp trong mẫu

Loại hình sỡ hữu	Số lượng	Tỷ lệ	Số năm hoạt động	Số lượng	Tỷ lệ
Doanh nghiệp tư nhân trong nước	218	68.1%	<5	114	36%
FDI	44	13.8%	5–10	75	23%
Doanh nghiệp nhà nước	19	6%	10–20	64	20%
Tổ chức phi chính phủ	1	0.3%	>20	67	21%
Cơ quan sự nghiệp	11	3.4%	Tổng	320	100%
Tổ chức khác	27	8.4%			
Tổng	320	100%			
Loại hình kinh doanh			Quy mô (nhân viên)		
Thương mại	77	24%	<50	123	38%
Dịch vụ	100	31%	50–150	79	25%
Sản xuất	33	10%	150–300	37	12%
Dịch vụ công	9	3%	300–1.000	45	14%
Khác	101	32%	>1.000	36	11%
Tổng	320	100%	Tổng	320	100%

4. Kết quả nghiên cứu

4.1. Phân tích pre-test

Để đánh giá hiện tượng chệch do không phản hồi (Non-response Bias Test – NBT), nhóm tác giả đã tiến hành phân tích *t*-test trên SPSS. Kết quả cho thấy không có sự khác biệt có ý nghĩa thống kê trong trung bình tổng thể giữa nhóm trả lời sớm và trả lời muộn (Armstrong & Overton, 1977) giữa 90% người phản hồi sớm nhất so với 10% người phản hồi trễ nhất trong khảo sát. Do đó, NBT không tồn tại trong nghiên cứu này.

Để kiểm tra tính vững chắc của dữ liệu, nghiên cứu thực hiện kiểm tra hiện tượng biến thiên do phương pháp (Common Method Variance – CMV) và tính không đồng nhất chưa được quan sát (Unobserved Heterogeneity – UNH) của dữ liệu. CMV được kiểm tra bằng kiểm định đơn nhân tố của Harman. Kết quả phân tích EFA (Exploratory Factor Analysis) đơn nhân tố cho thấy một nhân tố chỉ chiếm 38,23% tổng phương sai, chứng minh rằng CMV không phải là một vấn đề nghiêm trọng (Podsakoff và cộng sự, 2012) . Kỹ thuật FIMIX-PLS được sử dụng để kiểm tra UNH (Hair và cộng sự, 2017). Kết quả phân tích dừng lại ở giải pháp phân mẫu thành hai nhóm vì kích thước của giải

pháp phân mẫu thành ba nhóm là rất nhỏ (5,5%), thấp hơn ngưỡng của một nhóm hợp lý là 25%, cho thấy UNH là không tồn tại.

Các kết quả phân tích tác động phi tuyến bằng kỹ thuật tạo biến Quadratic Effect cho các biến ngoại sinh chỉ ra rằng các hiệu ứng phi tuyến không tồn tại trong dữ liệu vì tác động bậc hai của các biến ngoại sinh trong mô hình là không đáng kể (Hair và cộng sự, 2017).

4.2. Kiểm tra mô hình đo lường

Mô hình đo lường sau có tất cả các hệ số tải nằm trong khoảng từ 0,737 đến 0,995 (Hair và cộng sự, 2017) và phương sai trích trung bình (Average Variance Extracted – AVE) từ 0,597 đến 0,946, cao hơn ngưỡng tối thiểu 0,5 (Fornell & Larcker, 1981) (Bảng 2). Giá trị hội tụ cũng được xác nhận thông qua thống kê *t* đối với mỗi hệ số tải nếu chúng có ý nghĩa thống kê. Trong nghiên cứu này, hệ số tải của từng biến quan sát có ý nghĩa ở mức p <0,001. Tất cả hệ số CA (Cronbach's Alpha) và hệ số CR (Composite Reliability) đều đạt giá trị cao hơn 0,7 (Hair và cộng sự, 2017). Do đó, giá trị hội tụ và độ tin cậy của các biến quan sát và cấu trúc đã đạt được.

Bảng 2.

Kết quả đánh giá mô hình đo lường

Cấu trúc		Tính ổn định nội bộ		AVE
	Hệ số tải	CA	CR	
CSRD	0,951 - 0,968	0,958	0,973	0,923
CSRI	0,909 - 0,929	0,911	0,944	0,850
CSRP	0,915 - 0,935	0,913	0,945	0,852
CSRRc	0,968 - 0,971	0,936	0,969	0,940
CSRRs	0,954 - 0,960	0,954	0,970	0,916
EC	0,737 - 0,807	0,868	0,899	0,597
MRB	0,950 - 0,995	0,955	0,972	0,946
OSP	0,841 - 0,934	0,942	0,956	0,813
SETA	0,888 - 0,920	0,944	0,957	0,816
SI	0,918 - 0,948	0,932	0,956	0,880
TAB	0,967 - 0,968	0,931	0,967	0,935
TAM	0,902 - 0,925	0,903	0,939	0,838

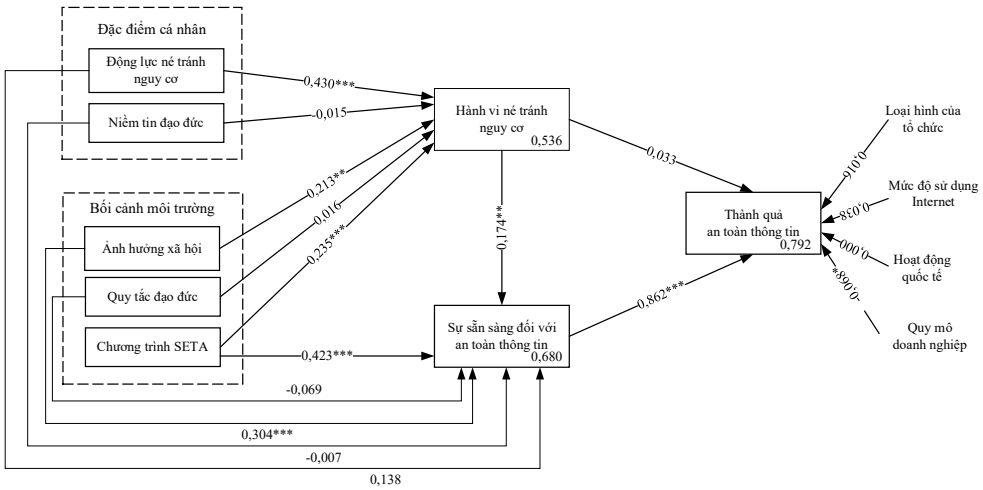
Bảng 3 cho thấy tất cả các giá trị HTMT của các cấu trúc đều nhỏ hơn 1 (Henseler và cộng sự, 2016). Hệ số Fornell và Larcker của các cấu trúc tại đường chéo là cao nhất so với các hệ số tại các cấu trúc khác (Fornell & Larcker, 1981). Hệ số tải chéo của các biến quan sát là cao nhất tại cấu trúc của nó so với các cấu trúc khác. Kết quả này chứng minh giá trị phân biệt của tất cả các cấu trúc đã thỏa mãn.

Bảng 3.
Giá trị HTMT

	CSRD	CSRI	CSRP	CSRRc	CSRRs	EC	MRB	OSP	SETA	SI	TAB
CSRI	0,908										
CSRP	0,945	0,924									
CSRRc	0,908	0,847	0,873								
CSRRs	0,952	0,900	0,885	0,975							
EC	0,274	0,275	0,314	0,266	0,290						
MRB	0,032	0,040	0,054	0,051	0,028	0,330					
OSP	0,894	0,858	0,871	0,902	0,910	0,257	0,026				
SETA	0,732	0,691	0,677	0,650	0,721	0,382	0,059	0,699			
SI	0,686	0,732	0,744	0,644	0,658	0,324	0,048	0,663	0,539		
TAB	0,669	0,708	0,649	0,605	0,615	0,340	0,051	0,637	0,553	0,648	
TAM	0,613	0,632	0,669	0,531	0,565	0,423	0,064	0,560	0,441	0,690	0,721

4.3. Kiểm tra mô hình cấu trúc

Kết quả phân tích Bootstrapping 5.000 lần được tổng hợp trong Hình 2 cho thấy CSR (β = 0,862; p < 0,0001) ảnh hưởng đáng kể đến OSP, do đó giả thuyết H_2 được chấp nhận. Các tiền tố của hành vi né tránh nguy cơ bao gồm động lực né tránh nguy cơ (β = 0,430; p < 0,0001), SETA (β = 0,235; p < 0,0001), và ảnh hưởng xã hội (β = 0,213; p < 0,001). Kết quả này ủng hộ giả thuyết H_{4a}, H_{8a} và H_{6a}. Các yếu tố quan trọng tác động đến CSR bao gồm SETA (β = 0,423; p < 0,0001), ảnh hưởng xã hội (β = 0,304; p < 0,0001), và hành vi né tránh nguy cơ (β = 0,174; p < 0,001) (các giả thuyết H_{8b}, H_{6b}, và H_3 được chấp nhận). Quy mô doanh nghiệp có ảnh hưởng đến OSP (β = 0,068; p < 0,05).



*** p < ,0001.; ** p < ,001; * p < 0,05

Hình 2. Kết quả kiểm tra mô hình cấu trúc

Kết quả phân tích ở Bảng 4 cho thấy CSR đóng vai trò là trung gian toàn phần cho tác động từ hành vi né tránh nguy cơ đến OSP. Trong các mối quan hệ thì hành vi né tránh nguy cơ là trung gian toàn phần cho tác động của động lực né tránh nguy cơ đến CSR.

Bảng 4.

Kết quả phân tích biến trung gian

	Tác động trực tiếp			**Tác động gián tiếp**			*Vai trò trung gian*
	Hệ số đường dẫn (β)	*P Values*	*Mức ý nghĩa (sig,)*	*Hệ số đường dẫn (β)*	*P Values*	*Mức ý nghĩa (sig,)*	
TAB → CSR → OSP	0,033	0,419	Không	0,150	0,009	Có	Toàn phần
TAM → TAB → CSR	0,138	0,067	Không	0,075	0,005	Có	Toàn phần
EC → TAB → CSR	-0,069	0,115	Không	0,000	0,993	Không	Không
SETA → TAB → CSR	0,423	0,000	Có	0,041	0,069	Không	Không
SI → TAB → CSR	0,304	0,000	Có	0,037	0,070	Không	Không
MRB → TAB → CSR	-0,007	0,837	Không	-0,003	0,707	Không	Không

4.4. Phân tích post-hoc

Kết quả kiểm tra hệ số xác định R^2 cho thấy mô hình cấu trúc có khả năng giải thích cao. Cụ thể, các cấu trúc ngoại sinh có khả năng giải thích lần lượt là 79,2%, 68% và 53,6% biến thiên của OSP, CSR, và hành vi né tránh nguy cơ (Hình 2). Hệ số tác động f^2 của CSR là 1,906, thể hiện tác động mạnh của nó đến OSP. Các yếu tố bao gồm SETA (f^2 = 0,359) và ảnh hưởng của xã hội (f^2 = 0,144) tác động mạnh đến CSR. Hành vi né tránh nguy cơ (f^2 = 0,044) và động lực né tránh nguy cơ (f^2 = 0,027) có tác động yếu đến CSR. Đối với biến nội sinh là hành vi né tránh nguy cơ thì biến có ảnh hưởng mạnh là động lực né tránh nguy cơ (f^2 = 0,218), biến có tác động trung bình yếu bao gồm SETA (f^2 = 0,083) và ảnh hưởng của xã hội (f^2 = 0,051) (Chin, 1998).

Hệ số Q^2 của OSP, CSR, và hành vi né tránh nguy cơ lần lượt là 63,4%, 53,1%, và 48,4%. Chỉ số này đều lớn hơn 0, do đó mô hình có khả năng dự báo tốt bởi các biến ngoại sinh. Kết quả phân tích cho thấy VIF đối với các biến độc lập cao hơn 0,20 (thấp hơn 5), điều này chứng minh rằng đa cộng tuyến không tồn tại giữa các biến độc lập. Bên cạnh đó, nhóm tác giả sử dụng chỉ số SRMR để đánh giá mức độ phù hợp của mô hình. Hệ số SRMR hiện tại là 0,045, dưới giới hạn trên là 0,10; do đó, mô hình nghiên cứu có tính phù hợp cao (Hair và cộng sự, 2017).

5. Thảo luận

Nghiên cứu này đã khám phá cơ chế tác động của hành vi né tránh nguy cơ đến OSP thông qua vai trò trung gian toàn phần của CSR. Theo đó, khi các cá nhân thể hiện hành vi né tránh nguy cơ sẽ góp phần thúc đẩy sự sẵn sàng của tổ chức đối với ISe, củng cố cho lý thuyết ORC (Weiner, 2020). Đồng thời CSR ảnh hưởng tích cực đến OSP. Khám phá này phù hợp với quan điểm của Hasan và

cộng sự (2021). Đây là một phát hiện quan trọng, nhấn mạnh vai trò của CSR nhằm thay đổi và ứng phó với nguy cơ trong toàn tổ chức, từ đó góp phần gia tăng OSP. Kết quả này cũng cho thấy hành vi né tránh nguy cơ không ảnh hưởng trực tiếp đến OSP, điều này có thể được giải thích bởi bản chất phức tạp của ISe, vốn đòi hỏi một nền tảng tổ chức vững chắc – bao gồm chính sách, đào tạo, và văn hóa an toàn – để chuyển hóa các hành vi né tránh nguy cơ thành kết quả. Hành vi né tránh nguy cơ, dù quan trọng, không thể tự thân tạo ra thành quả nếu thiếu sự hỗ trợ từ một hệ thống sẵn sàng. Do đó, sự sẵn sàng đóng vai trò như một cầu nối thiết yếu, khuếch đại tác động của hành vi né tránh nguy cơ, từ đó nâng cao OSP.

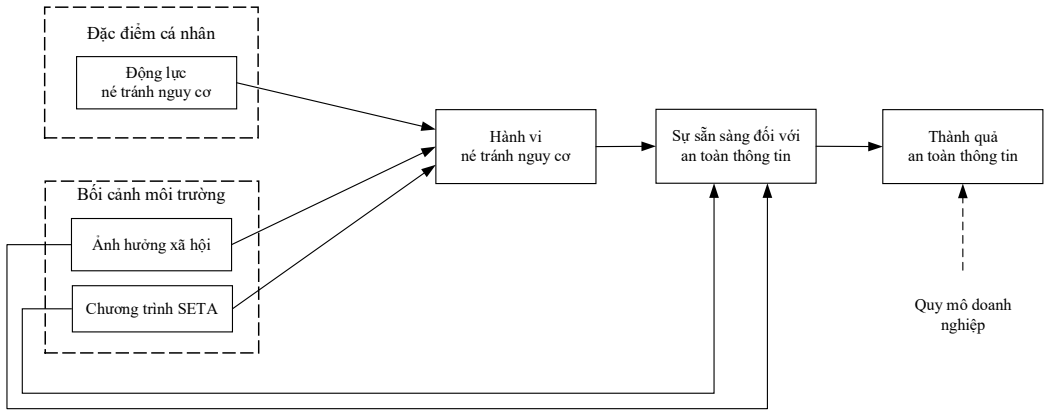
Nghiên cứu cho thấy động lực né tránh nguy cơ là đặc điểm cá nhân có ảnh hưởng trực tiếp và đáng kể đến hành vi né tránh nguy cơ. Phát hiện này củng cố các quan điểm của lý thuyết PMT và lý thuyết kỳ vọng, cũng như phù hợp nghiên cứu của Carpenter và cộng sự (2019). Đồng thời, động lực né tránh nguy cơ cũng gián tiếp thúc đẩy CSR thông qua vai trò trung gian toàn phần của hành vi né tránh nguy cơ. Cơ chế này cho thấy rằng, chỉ khi cá nhân thực sự hình thành hành vi cụ thể; ví dụ, cập nhật phần mềm bảo mật, hay tuân thủ quy trình xác thực đa yếu tố, thì mới có thể góp phần làm tăng mức độ sẵn sàng chung của tổ chức. Tuy nhiên, niềm tin đạo đức không cho thấy tác động đáng kể nào, điều này trái với phát hiện của Chatterjee và cộng sự (2015). Thực tế, để niềm tin đạo đức thúc đẩy hành vi, cá nhân cần xây dựng "bản sắc đạo đức" liên tục được nuôi dưỡng qua đào tạo và văn hóa doanh nghiệp; nếu thiếu sự hỗ trợ này, niềm tin dù mạnh cũng khó dẫn dắt hành động. Trong bối cảnh Việt Nam – xã hội theo văn hóa Á Đông với đặc trưng tập thể và khoảng cách quyền lực cao, các quyết định về ISe thường bị chi phối bởi cơ chế kiểm soát tập trung và nỗi lo ngại về khen thưởng, kỷ luật hơn là chuẩn mực đạo đức cá nhân. Điều này khác với văn hóa phương tây, nơi cá nhân thường chủ động hành động theo giá trị đạo đức nội tại.

Ảnh hưởng xã hội và SETA là hai trong số ba yếu tố môi trường trực tiếp thúc đẩy hành vi né tránh nguy cơ và đồng thời nâng cao mức độ sẵn sàng của tổ chức đối với ISe. Điều này nhất quán với các lý thuyết như TPB, PMT và lý thuyết học tập xã hội, cho thấy hành vi cá nhân không chỉ là kết quả của động lực nội tại mà còn bị chi phối mạnh mẽ bởi các yếu tố bên ngoài, đặc biệt là nhận thức về sự kỳ vọng và hành vi của những người xung quanh. Khi cá nhân thường xuyên tiếp xúc, trao đổi về các tình huống rủi ro với đồng nghiệp hoặc lãnh đạo, họ dễ hình thành niềm tin và thói quen né tránh rủi ro hơn, từ đó lan tỏa thành năng lực chung của tổ chức. SETA không chỉ cung cấp kiến thức mà còn tạo ra môi trường thực hành, củng cố nhận thức và kỹ năng an toàn, giúp nhân viên chủ động thực hiện các biện pháp bảo vệ thông tin, góp phần làm tăng mức độ sẵn sàng phòng ngừa nguy cơ. Phát hiện này bổ sung bằng chứng thực nghiệm trước (Puhakainen & Siponen, 2010), đồng thời cho thấy đầu tư vào đào tạo nhân viên là yếu tố thiết yếu để nâng cao OSP.

Quy tắc đạo đức không ảnh hưởng đáng kể đến hành vi né tránh nguy cơ và mức độ sẵn sàng với ISe. Điều này có thể lý giải bởi tính chung chung của các bộ quy tắc: chúng thường được ban hành dưới dạng văn bản, thiếu cơ chế truyền thông tương tác và ít gắn với tình huống thực tế, nên nhân viên khó nhìn thấy mối liên hệ trực tiếp giữa các quy tắc đạo đức và hành động cụ thể (Rosenberg, 1998), do đó, chúng không tự động chuyển thành hành vi an toàn nếu thiếu các quy định và cơ chế kiểm soát hỗ trợ (Siponen & Willison, 2009).

Hàm ý quản trị

Nghiên cứu này đã phát triển một khuôn mẫu đánh giá OSP (Hình 3). Trong đó OSP bị chi phối trực tiếp và mạnh mẽ bởi CSR. Hành vi né tránh nguy cơ của nhân viên cùng với ảnh hưởng của xã hội và SETA có những tác động đáng kể đến CSR của doanh nghiệp.



Hình 3. Khuôn mẫu đánh giá thành quả an toàn thông tin

Trong bối cảnh phức tạp và nghiêm trọng của các nguy cơ ISe, nhà quản trị cần tập trung vào những chiến lược mạnh mẽ nhằm nâng cao OSP, từ đó hỗ trợ mục tiêu phát triển doanh nghiệp. Kết quả của nghiên cứu này đã chứng minh vai trò quan trọng của CSR đối với OSP, gợi mở những định hướng cải thiện OSP. Cụ thể, để gia tăng CSR, doanh nghiệp cần tập trung đẩy mạnh sự nhận biết, giải pháp bảo vệ, phát hiện, phản ứng, và phục hồi sau sự cố và thảm họa ISe. Sự nhận biết có thể được tăng cường bằng cách sử dụng các phương pháp tiên tiến để đánh giá các điểm yếu tiềm ẩn, kiểm soát các cổng máy tính có thể được sử dụng để tấn công và cần đảm bảo rằng các điểm yếu tiềm ẩn của hệ thống nằm trong mức độ chấp nhận rủi ro. Các vấn đề cần quan tâm đối với các giải pháp bảo vệ hệ thống thông tin bao gồm mã hóa dữ liệu tại các thiết bị đầu cuối, phần mềm diệt virus, và thực thi chính sách mật khẩu mạnh. Chủ động quản lý các nguy cơ mới trước khi chúng xảy ra, thực hiện các phân tích mang tính chiến lược về các sự cố an toàn đã xảy ra, và liên tục theo dõi các cảnh báo an toàn để phát hiện các cuộc tấn công mạng cũng là các biện pháp cần triển khai. Doanh nghiệp cũng cần sẵn sàng ứng phó với các cuộc tấn công tiềm ẩn, thiết lập hệ thống để giám sát việc chuyển đổi dự phòng, và lập kế hoạch phục hồi sau các cuộc tấn công mạng. Cuối cùng, sự sẵn sàng trong cam kết có các quy trình thực hiện kế hoạch phục hồi sau sự cố và thảm họa ISe cũng như khắc phục sự cố thông qua việc lưu giữ và cập nhật cơ sở dữ liệu sao lưu cần được triển khai.

Kết quả nghiên cứu đã chứng minh rằng hành vi né tránh nguy cơ ảnh hưởng đáng kể trực tiếp đến CSR và gián tiếp đến OSP. Do đó, các hành động nhằm củng cố CSR nên tập trung cũng bao gồm việc thực hiện và thường xuyên cập nhật các thủ tục về ISe. Những giải pháp nhằm cải thiện động lực né tránh nguy cơ của nhân viên, SETA, và ảnh hưởng xã hội nên được ưu tiên bởi vì chúng có tác động cả trực tiếp và gián tiếp đến CSR thông qua hành vi né tránh nguy cơ.

Những tác động của ảnh hưởng của xã hội đến sự sẵn sàng của ISe trong doanh nghiệp cho thấy, các chiến lược của cơ quan chính phủ và tổ chức tư vấn về ISe cần thực hiện là tạo ra môi trường xã hội quan tâm đến ISe như gia tăng truyền thông về ISe, từ đó phát huy hiệu quả trong cải thiện OSP.

6. Kết luận

Trong bối cảnh các nguy cơ ISe ngày càng tăng, bên cạnh chiến lược tập trung vào công nghệ, vấn đề con người cũng cần được quan tâm. Kết hợp các lý thuyết gồm ORC, PMT, né tránh nguy cơ về công nghệ, động lực bảo vệ, học tập xã hội, và ra quyết định có đạo đức cùng các nghiên cứu thực nghiệm trước, nhóm tác giả đã kiểm tra một mô hình đường dẫn về OSP và các tiền tố của nó. Kết quả phân tích PLS đã cung cấp bằng chứng về vai trò trung gian toàn phần của CSR cho tác động của hành vi né tránh nguy cơ đến OSP. Nhóm tác giả cũng xác nhận rằng hành vi né tránh nguy cơ là trung gian toàn phần cho tác động của động lực né tránh nguy cơ đến CSR của doanh nghiệp. Ngoài ra, các phân tích dữ liệu cũng chứng minh tác động trực tiếp của SETA và ảnh hưởng xã hội đến CSR. Vì những hậu quả nghiêm trọng do các nguy cơ ISe gây ra cho doanh nghiệp đang ngày càng gia tăng, nên những đóng góp của nghiên cứu này là đáng kể.

Nghiên cứu này tồn tại một số hạn chế gợi mở các hướng nghiên cứu tiếp theo. Thứ nhất, nghiên cứu khảo sát dữ liệu tại một thời điểm; do đó, các giải thích về mối quan hệ nhân quả của các cấu trúc trong mô hình nên được sử dụng một cách cẩn trọng. Các nghiên cứu tiếp theo nên dựa trên dữ liệu theo thời gian. Thứ hai, nhóm tác giả tập trung vào một số yếu tố có thể tác động đến OSP như CSR và hành vi né tránh nguy cơ, vì vậy, kết quả giải thích cho biến thiên của OSP chưa quá cao. Nghiên cứu trong tương lai nên mở rộng mô hình nhằm tăng cường khả năng giải thích OSP. Cuối cùng, tác động của OSP đến thành quả hoạt động tài chính và phi tài chính của doanh nghiệp cũng nên được xem là một định hướng nghiên cứu.

Tài liệu tham khảo

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

Bandura, A., & Walters, R. H. (1977). *Social Learning Theory* (Vol. 1). Prentice hall Englewood Cliffs, NJ.

Burns, A., Roberts, T. L., Posey, C., Bennett, R. J., & Courtney, J. F. (2018). Intentions to comply versus intentions to protect: A VIE theory approach to understanding the influence of insiders' awareness of organizational SETA efforts. *Decision Sciences*, *49*(6), 1187-1228.

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining technology threat avoidance theory. *Communications of the Association for Information Systems*, *44*.

Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems*, *31*(4), 49-87.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern Methods for Business Research*, *295*(2), 295-336.

Cisco Systems, I. (2023). *Cybersecurity Readiness Index.* In: Cisco.

D'Arcy, J., & Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sciences*, *43*(6), 1091-1124.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79-98.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, *35*(8), 982-1003.

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: A ten-year update. *Journal of Management Information Systems*, *19*(4), 9-30.

Ernest C., S., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, *106*(3), 345-361.

Federal Bureau of, I. (2023). *Internet Crime Report 2022*. Retrieved from https://www.ic3.gov/AnnualReport/Reports/2022_ic3report.pdf?utm_source=chatgpt.com

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.

Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2017). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)* (2 ed.). Sage Publications.

Hair, J. F., Sarstedt, M., Ringle, C. M., & Gudergan, S. P. (2017). *Advanced Issues in Partial Least Squares Structural Equation Modeling*. Sage Publications.

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*, 102726.

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.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549-566.

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.

Lankton, N. K., Stivason, C., & Gurung, A. (2019). Information protection behaviors: morality and organizational criticality. *Information & Computer Security*, *27*(3), 468-488.

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., & Hohler, B. (2013). *Employees' information security awareness and behavior: A literature review*. 2013 46th Hawaii International Conference on System Sciences.

Lee, S. M., Lee, S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*, *41*(6), 707-718.

Liang, & Xue. (2009). Avoidance of information technology threats: A theoretical Perspective. *MIS Quarterly*, *33*(1), 71-90.

Lincoln, S. H., & Holmes, E. K. (2011). Ethical decision making: A process influenced by moral intensity. *Journal of Healthcare, Science and the Humanities*, *1*(1), 55-69.

Meltzer, J. P. (2020). Cybersecurity, digital trade, and data flows: Re-thinking a role for international trade rules. https://www.brookings.edu/articles/cybersecurity-digital-trade-and-data-flows-re-thinking-role-for-international-trade-rules/?utm_source=chatgpt.com

Molander, E. A. (1987). A paradigm for design, promulgation and enforcement of ethical codes. *Journal of Business Ethics*, *6*, 619-631.

NCSGroup. (2025). *Báo cáo an ninh mạng 2024*. Truy cập từ https://ncsgroup.vn/wp-content/uploads/2025/01/NCS-Bao-cao-an-ninh-mang-2024.pdf

Nemati, H. (2007). *Information security and ethics: concepts, methodologies, tools, and applications: concepts, methodologies, tools, and applications*. IGI global.

Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2012). Sources of method bias in social science research and recommendations on how to control it. *Annual Review of Psychology*, *63*, 539-569.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, *34*(4), 757-778.

Rashotte, L. (2007). Social Influence. In *The Blackwell Encyclopedia of Sociology*. https://doi.org/10.1002/9781405165518.wbeoss154

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

Rîndașu, S. M. (2017). Emerging information technologies in accounting and related security risks–what is the impact on the Romanian accounting profession. *Journal of Accounting and Management Information Systems*, *16*(4), 581-609.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology*, *91*(1), 93-114.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In *Social psychology: A Sourcebook*, (pp.153-176). Guilford

Rosenberg, R. S. (1998). *Beyond the code of ethics: The responsibility of professional societies.* Proceedings of the Ethics and Social Impact Component on Shaping Policy in the Information Age, https://doi.org/10.1145/276755.276768

Samtani, S., Zhu, H., & Yu, S. (2019). Fear appeals and information security behaviors: An empirical study on Mechanical Turk. *AIS Transactions on Replication Research*, *5*(1), 5.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, *46*(5), 267-270. https://doi.org/https://doi.org/10.1016/j.im.2008.12.007

Vance, A., & Siponen, M. T. (2012). IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing (JOEUC)*, *24*(1), 21-41.

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, *36*(1), 157-178.

Vroom, V. (1964). *Work and Motivation.* Wiley and Sons, New York.

Weiner, B. J. (2020). A theory of organizational readiness for change. In *Handbook on Implementation Science* (pp. 215-232). Edward Elgar Publishing.

Whitman, & Mattord. (2022). *Principles of Information Security* (7 ed.). Cengage Learning, Inc.

Young, D. K., Carpenter, D., & McLeod, A. (2016). Malware avoidance motivations and behaviors: A technology threat avoidance replication. *AIS Transactions on Replication Research*, *2*(1), 8.