ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC QUỐC TẾ

Tên đề tài:

KHAI PHÓNG TIỀM NĂNG TRUYỀN THÔNG CHÍNH PHỦ VÀ CHÍNH SÁCH AN NINH MẠNG CỦA TỔ CHỨC: VAI TRÒ CỦA CÁC NHÂN TỐ CHÍNH ẢNH HƯỞNG ĐẾN HÀNH VI BẢO VỆ AN NINH MẠNG CỦA NHÂN VIÊN

LUẬN ÁN TIẾN SĨ

TRẦN VĂN DIỄN

PPMIU22002

CHUYÊN NGÀNH: QUẢN LÝ CÔNG

Mã số chuyên ngành: 9340403

NGƯỜI HƯỚNG DẪN KHOA HỌC:
PGS.TS. NGUYỄN VĂN PHƯƠNG

TP.HỒ CHÍ MINH, 2024

CHƯƠNG I. GIỚI THIỆU

Định nghĩa:

"An ninh mạng (*cybersecurity*) là việc bảo vệ hệ thống mạng máy tính khỏi các hành vi trộm cắp danh tính, dữ liệu hoặc làm tổn hại đến phần cứng, phần mềm và các nguyên nhân dẫn đến sự gián đoạn của máy tính (Gasser., 1988)"; vấn để đảm bảo ANM cần phải đảm bảo cùng lúc trên cả lĩnh vực an ninh máy tính (*computer security*) và lĩnh vực bảo mật công nghệ thông tin (*IT security*)".

Bảo vệ An ninh mạng là việc các cơ quan tổ chức triển khai các biện pháp nhằm đảm bảo ANM cho tổ chức mình như: mạng lưới máy tính, hệ thống điện tử, thiết bị di động, chương trình và dữ liệu của hệ thống máy tính khỏi các cuộc tấn công của nhóm tội phạm công nghệ *(TPCN:hacker)* bằng mã độc và có chủ đích nhằm vào hệ thống cơ sở hạ tầng mạng máy tính của cơ quan tổ chức, khi họ tham gia vào các hoạt động trên không gian mạng. Tội phạm trên không gian mạng gọi chung là TPCN (hacker) có thể thực hiện một loạt các vụ tấn công vào mạng máy tính của cơ quan tổ chức hoặc cá nhân nhằm kiểm soát quyền truy cập, điều khiển máy tính để nhằm mục đích biến đổi, trộm cắp hoặc xóa bỏ dữ liệu; với nhiều mục đích khác nhau như: về kinh tế, can dự trực tiếp vào các quy định, hoạch định trong quản lý hay kinh doanh, tống tiền hay an ninh chính trị, ….

1.1 Bối cảnh nghiên cứu

Với sự phát triển của kỷ nguyên 4.0, hầu hết các công ty đang thực hiện chuyển đổi số để duy trì cạnh tranh (Demirbas et at., 2018; Salunke et at., 2019). Chuyển đổi số và gia công dịch vụ CNTT đóng vai trò quan trọng, khiến an ninh mạng trở thành mối quan tâm lớn khi nguy cơ bị tấn công mạng và vi phạm dữ liệu tăng cao (Gozman & Willcocks., 2019; Makridis & Dean., 2018).

Việt Nam đang phát triển nhanh chóng về công nghệ thông tin. Theo Liên minh Viễn thông Quốc tế (ITU), Việt Nam đứng thứ 9 thế giới về số người dân thành thạo công nghệ số với 7,5 triệu người. Báo cáo của WIPO xếp Việt Nam ở vị trí 48/132 quốc gia về chỉ số đổi mới sáng tạo toàn cầu năm 2022, đặc biệt trong kỹ thuật số dựa trên siêu máy tính, trí tuệ nhân tạo (AI) và tự động hóa. Hiện nay, Chính phủ Việt Nam đang thúc đẩy xây dựng Chính phủ số để cải cách hành chính, nhưng vẫn còn nguy cơ tiềm ẩn nhiều rủi ro thách thức về ANM.

Tại Việt Nam, đã xuất hiện nhiều cuộc tấn công mạng nhằm vào các cơ sở hạ tầng thông tin trọng yếu của Chính phủ và các tổ chức lớn ngày càng phức tạp và nguy hiểm. Theo Bộ Công an, mỗi năm có hàng nghìn trang mạng Việt Nam bị tin tặc tấn công nhằm đánh cắp thông tin và cài mã độc. Trong 6 tháng đầu năm 2019, đã có hơn 2.500 trang tin và cổng thông tin điện tử Việt Nam bị tấn công, và hàng trăm ngàn máy tính bị nhiễm mã độc. Việt Nam đứng thứ 4 trong 10 quốc gia bị kiểm soát bởi mạng botnet.

Không gian mạng và an ninh mạng là lĩnh vực mới, đang phát triển nhanh chóng hơn tốc độ nghiên cứu khoa học (Dawson & Thomson., 2018). Lĩnh vực này không chỉ đối mặt với thách thức công nghệ mà còn bị chi phối bởi hành vi con người. Dù các chuyên gia công nghệ đóng vai trò quan trọng, nhưng không thể đảm bảo ANM hoàn toàn hiệu quả. Con người cũng giữ vai trò then chốt, với hơn 70% vụ vi phạm hệ thống hoặc dữ liệu thành công là do lỗi con người (IBM Global Technology Services., 2014; Carlton & Levy., 2015).

Tháng 2/2023 Cục Công nghệ thông tin H05 BCA phát hiện biến thể mã độc gián điệp mới xuất hiện trong mạng máy tính nội bộ của BCA, thu thập các tài liệu (.doc. docx, xlsx, ppt, pdf) tự động mã hóa tập tin hay copy ra thiết bị lưu trữ ngoài, tìm kiếm kết nối internet để truyền data đã thu thập về máy chủ được đặt tại nước ngoài. Các nhóm tin tặc thực hiện cải tiến thêm

module soạn thảo văn bản để đánh lừa người dùng, đây là biến thể mã độc gián điệp vượt qua cơ chế nhận diện của nhiều phần mềm phòng, chống virus, mã độc.

Theo báo cáo tình hình TPCN các năm gần đây 2020, 2021, 2022, và 2023 của Bộ Công an nhóm TPCN ngày này đang gia tặng nhanh về số lượng và cả số vụ; các cuộc tấn công an ninh, an toàn thông tin của tin tặc ngày càng đa dạng trên mọi lĩnh vực và khía cạnh khác nhau; theo (Maglaras et al., 2019) mục tiêu chính của các cuộc tấn công mạng là Cấu trúc cơ sở hạ tầng quốc gia quan trọng (CNI) của một quốc gia như cảng, bệnh viện, nhà sản xuất nước, khí đốt hoặc điện, sử dụng và dựa vào giám sát điều khiển và thu thập dữ liệu (SCADA) và Hệ thống kiểm soát thử nghiệm công nghiệp (ICS) để quản lý hoạt động sản xuất của họ. Việc bảo vệ CNI trở thành một vấn đề thiết yếu cần được xem xét.

Tổng kết về công tác bảo vệ bí mật nhà nước năm 2023, Chính phủ đã phát hiện lộ bí mật nhà nước thông qua không gian mạng (như: mạng Zalo, email, trang thông tin điện tử,…) của các cơ quan, ban ngành chính phủ, từ Trung ương tới địa phương đã vô ý làm lộ 3.184 tài liệu trong đó có 2000 tài liệu tuyệt mật; 06 tháng đầu năm 2023 Bộ Công an phát hiện lộ BMNN 236 tài liệu có nội dung chưa BMNN thuộc Bộ Công an và Bộ Quốc phòng được truyền qua đường truyền viễn thông không mã hóa (226 tài liệu liên quan đến an ninh quốc phòng).

Để duy trì hoạt động kinh doanh và bảo vệ thông tin trong không gian mạng, hành vi an ninh mạng của nhân viên là chìa khóa (Li et at., 2019). Dù được quan tâm, nghiên cứu về ANM vẫn chưa được khai thác hiệu quả tại các quốc gia có nền kinh tế đang phát triển. Tại Việt Nam, đã có nghiên cứu về ANM nhưng chủ yếu sử dụng phương pháp tiếp thị xã hội liên ngành để kiểm tra cách nhân viên trải nghiệm và tuân thủ các sáng kiến bảo mật (Pham et at., 2019).

Nghiên cứu này sẽ khám phá hiệu quả đổi mới và sáng tạo của các nhà cung cấp dịch vụ CNTT và ANM tại Việt Nam trong bối cảnh toàn cầu hóa và không gian mạng. Dữ liệu được thu thập từ các nhà cung cấp CNTT, chuyên gia, và nhân viên trong lĩnh vực công qua các câu hỏi cấu trúc và phỏng vấn. Luận án sẽ sử dụng mô hình PLS-SEM để khám phá các nhân tố tác động đến nhận thức và hành vi ANM của nhân viên, đồng thời tìm hiểu cách họ đối phó với các mối đe dọa và nguy cơ mất an toàn CNTT.

Đảm bảo an ninh mạng và an ninh quốc gia không thể thực hiện riêng lẻ trong phạm vi vùng, miền, cơ quan tổ chức, hay cá nhân. Việc tuân thủ các biện pháp phòng chống ANM cần được thực hiện đồng bộ trên phạm vi toàn quốc, từ Trung ương đến địa phương. Vì vậy, nghiên cứu vấn đề ANM tại Việt Nam trong bối cảnh hiện nay là cần thiết để xác định các nguyên nhân mang tính hệ thống và toàn diện. Từ đó, có thể đề ra những giải pháp bảo đảm ANM mang tính cấp bách, chiến lược và phù hợp với thực tế quốc gia. Mà trong đó yếu tố con người cũng đóng vai trò rất quan trọng trong quá trình này.

1.2. Khoảng trống cần nghiên cứu

Đầu tiên, từ việc xem xét tổng thể các nghiên cứu trước, nhận thấy cần nghiên cứu kỹ lưỡng hơn về CSA của nhân viên và hành vi của họ trong việc bảo vệ hệ thống thông tin của tổ chức. Tuy nhiên, các học giả thường tập trung vào đánh giá ý định, thái độ hoặc khả năng xảy ra hành vi, điều này có thể không cung cấp hướng dẫn toàn diện cho các tổ chức muốn hiểu rõ tác động của nhận thức về bảo mật đối với hành vi của nhân viên (Anderson & Agarwal, 2010; Herath & Rao., 2009; Johnston & Warkentin., 2010; Ng et at., 2009; Siponen et at., 2014; Wu, 2020; Li et at., 2019, 2022). Vì vậy, trong luận án này, chúng tôi sẽ áp dụng lý thuyết PMT, lý thuyết TPB và lý thuyết CT để đánh giá tác động của CSA đối với IPM, ISPC, ATT, và hành vi bảo vệ an toàn thông tin của nhân viên. CSA sẽ được đánh giá thông qua năm biến số

chính của PMT: PS của mối đe dọa, PV trước mối đe dọa, RE, SE, và PB. Điều này sẽ giúp việc đo lường trở nên toàn diện hơn.

Thứ hai, việc xây dựng các văn bản chính sách pháp lý dựa trên tiêu chuẩn quốc tế có thể góp phần xây dựng văn hóa an toàn thông tin toàn diện cho mỗi tổ chức (Chen et at., 2015). Tuy nhiên, hiệu quả của các chính sách ANM vẫn chưa đạt được sự đồng thuận trong các nghiên cứu hiện tại. Một số học giả cho rằng chính sách ANM không có ảnh hưởng đáng kể đến ý định và hành vi lạm dụng máy tính, bao gồm sửa đổi, đánh cắp hoặc phá hủy phần mềm và dữ liệu (D'Arcy et at., 2009; Lee & Larsen., 2009). Mặc dù đã cung cấp chính sách và hướng dẫn bằng văn bản, một số nhân viên vẫn bỏ qua hoặc đánh giá thấp rủi ro (Han et at., 2017; Ifinedo., 2012, 2014; Li et at., 2019). Trước những kết quả trái ngược này, bài viết sẽ xem xét ảnh hưởng của các chính sách ANM của tổ chức đối với nhận thức và EPB ANM của nhân viên.

Thứ ba, các cơ quan chính phủ ngày càng tận dụng tài khoản truyền thông mạng xã hội để quản lý khủng hoảng (Guo et at., 2021). Tuy nhiên, các nghiên cứu hiện tại chủ yếu tập trung vào việc khám phá lý do người dân tham gia vào mạng xã hội của chính phủ (GSM) trong thời kỳ khủng hoảng và phân loại các chiến lược nhắn tin khẩn cấp của GSM (Tang et at., 2021). Điều này nêu bật sự thiếu sót trong việc kiểm tra tác động của GSM đối với người dân, đặc biệt là nhân viên. Ở Việt Nam, Bộ Thông tin và Truyền thông đã và đang tích cực tăng cường công tác giám sát, chủ động rà soát, đánh giá số liệu thống kê, đẩy mạnh tuyên truyền và cảnh báo trên các phương tiện thông tin đại chúng để người dùng biết và tránh nguy cơ bị tấn công mạng. Do đó, với việc triển khai lý thuyết CT làm khung lý thuyết, ảnh hưởng của phương GMS đối với CSA của nhân viên trong các tổ chức cũng nên được xem xét kỹ lưỡng hơn.

Các tổ chức công và doanh nghiệp tại Việt Nam đang dần số hóa và tích cực theo đuổi các chính sách số hóa để tối ưu hóa việc lưu thông và lưu trữ

thông tin. Tuy nhiên, việc thiếu các chính sách, nghị định và thông tư toàn diện của Chính phủ để điều phối cơ sở hạ tầng kỹ thuật giữa các cơ quan, tổ chức từ Trung ương đến địa phương đã buộc các cơ quan này phải cài đặt hệ thống và mạng máy tính một cách độc lập, dựa trên kiến thức và ngân sách sẵn có của họ. Cách tiếp cận này thiếu sự đánh giá chuyên sâu về các gói mua sắm và cung cấp cơ sở hạ tầng, dẫn đến những thiếu sót trong quản lý và sử dụng hệ thống máy tính, gây nguy cơ mất an toàn thông tin đáng kể. Quan trọng hơn, một số công chức mặc dù có kiến thức cơ bản về an ninh mạng nhưng lại không tuân thủ các quy định của cơ quan do thiếu các quy chế, thông tư và nghị định hướng dẫn. Việc này dẫn đến các hành vi không tuân thủ như sao chép dữ liệu chưa được kiểm chứng bằng ổ USB hoặc sử dụng máy tính trái quy định, gây nguy hiểm cho an ninh thông tin trong hệ thống máy tính của khu vực công. Do đó, luận án này là cần thiết để cung cấp cơ sở vững chắc cho lãnh đạo cấp cao của các cơ quan tổ chức và Chính phủ trong việc đưa ra các quyết định chiến lược về an ninh mạng. Nghiên cứu sẽ giúp khắc phục những thiếu sót trong quản trị, sử dụng và vận hành hệ thống mạng máy tính, đảm bảo an toàn thông tin và nâng cao hiệu quả hoạt động của các cơ quan công quyền.

Luận án này giới hạn phạm vi nghiên cứu liên quan đến ANM của các cơ quan tổ chức tại Việt Nam.

1.3. Lý do chọn đề tài và tính cấp thiết của đề tài

Maglaras et al. (2019) nhận xét rằng mục tiêu chính của nhóm tội phạm công nghệ *(hacker)* hiện nay nhằm tấn công mạng vào các cơ sở hạ tầng quốc gia quan trọng như: cảng, bệnh viện, nhà máy nước, khí đốt và điện, sử dụng hệ thống SCADA và ICS để quản lý hoạt động sản xuất. Do đó, việc bảo vệ CNI trở thành một vấn đề thiết yếu cần được xem xét. Nhìn chung, các biện pháp bảo vệ ANM hiện có được phân loại theo các khía cạnh pháp lý, kỹ thuật, tổ chức, xây dựng, năng lực và hợp tác.

Theo Chỉ số vị trí dịch vụ toàn cầu (GSLI) 2019, Việt Nam xếp thứ năm trong số 50 quốc gia hàng đầu về cung cấp dịch vụ gia công CNTT, dựa trên bốn yếu tố chính: khuyến khích tài chính, nhóm lực lượng lao động và kỹ năng, môi trường kinh doanh và sự cộng hưởng kỹ thuật số. Vì vậy, việc sử dụng các dịch vụ gia công CNTT của Việt Nam ngày càng hấp dẫn hơn đối với cả khách hàng quốc tế và trong nước nhờ hiệu quả chi phí và đội ngũ lao động chuyên nghiệp, có năng lực thích nghi cao với CNTT. Hơn nửa, môi trường kinh doanh cho ngành CNTT tại Việt Nam đã được cải thiện đáng kể nhờ các khoản đầu tư nước ngoài từ các ông lớn như Intel, IBM, Samsung, LG và Microsoft và các công ty mới khởi nghiệp sáng tạo.

Tuy nhiên, cùng với sự phát triển mạnh mẽ của các dịch vụ CNTT, an ninh mạng trở thành một thách thức thực sự đối với các tổ chức. Từ năm 2018 đến nay, Việt Nam đã chứng kiến hàng loạt vụ vi phạm dữ liệu và tấn công mạng làm gián đoạn các hoạt động kinh doanh và ảnh hưởng sấu đến kết quả kinh doanh. Các sự cố như việc hacker làm nghẽn mạch phát sóng đài VOV năm 2021 và tấn công cơ sở dữ liệu dân cư quốc gia năm 2023 là ví dụ điển hình. Hầu hết các doanh nghiệp phải chịu hậu quả từ các cuộc tấn công mạng này, một phần do hành vi an ninh mạng thiếu thận trọng của nhân viên; ví dụ, máy tính bị nhiễm virus, nhân viên quên đăng xuất khỏi hệ thống hoặc nhấp vào email lừa đảo (Ponsard & Grandclaudon, 2020). Những tình huống này xuất phát từ việc thiếu nhận thức và kiến thức về an ninh mạng của nhân viên (Gratian et al., 2018).

Theo báo cáo Tổng kết công tác bảo vệ bí mật nhà nước năm 2023 của Bộ Công an, các cơ quan ban ngành của Chính phủ từ Trung ương đến địa phương, bao gồm cả Bộ Công an và Bộ Quốc phòng, đã để lộ hàng nghìn tài liệu chứa bí mật nhà nước trên không gian mạng do không tuân thủ đúng các quy định về bảo vệ an toàn CNTT và ANM. Các nhóm tội phạm CNTT ngày càng gia tăng về số vụ và đa dạng về thủ đoạn phương thức hoạt động trên không gian mạng, chúng chủ yếu lợi dụng vào sự thiếu cảnh giác và thiếu hiểu

biết về an ninh mạng của người dùng, trong đó có cả cán bộ công chức, viên chức (điển hình như những vụ lừa đảo thông qua việc tội phạm công nghệ đánh cắp các tài khoản cá nhân người dùng mạng xã hội hoặc thông tin tài khoản ngân hàng để thực hiện hành vi tội phạm).

Tại báo cáo diễn đàn kinh tế số năm 2024 vừa qua nhằm củng cố phát triển tài chính - Ngân hàng tại Việt Nam, trong năm 2023 có khoảng 14 nghìn cuộc tấn công mạng và 16 nghìn phản ánh lừa đảo trực tuyến, gây thiệt hại về kinh tế khoảng hơn 390 nghìn tỷ chiếm 3,6% GDP.

Mặc dù hệ thống pháp luật và các thông tư, nghị định về ANM của Việt Nam đã được Chính phủ ban hành, nhưng vẫn chưa hoàn thiện và còn chồng chéo trong việc quản lý và thực hiện. Các quy định pháp luật chưa đảm bảo một môi trường an toàn trên không gian mạng cho mọi người dân.

Ngoài ra, Việt Nam là một nền kinh tế mới nổi có khả năng thích nghi cao với sự thay đổi công nghệ nhanh chóng, chính phủ vẫn đang gặp khó khăn trong việc đẩy mạnh nền kinh tế kỹ thuật số trong khi phải đối mặt với các mối đe dọa và kiểm soát tấn công mạng. Hầu hết các doanh nghiệp từ các nước phát triển đầu tư rất nhiều vào an ninh mạng vì lo ngại xảy ra thảm họa bất ngờ như tin tặc, vi-rút hoặc xâm nhập phần mềm, nhưng hoạt động này rất tốn kém (Dreibelbis et at., 2018).

Dù chủ đề ANM nhận được sự yêu thương chăm sóc trong nhiều nghiên cứu gần đây, nhưng vẫn chưa được khai thác hiệu quả tại các quốc gia có nền kinh tế đang phát triển, đặc biệt là từ góc độ nhận thức và hành vi tại Việt Nam. Chính những lý do này đã thúc đẩy tác giả chọn chủ đề này làm luận án nghiên cứu.

2. Cơ Sở Lý Thuyết và khái niệm liên quan

2.1. Lý thuyết Động cơ Bảo vệ (*Protection motivation theory- PMT*)

Lý thuyết Động cơ Bảo vệ (PMT) bắt nguồn từ các lý thuyết về giá trị kỳ vọng, cho rằng hành động cụ thể có thể dẫn đến các kết quả nhất định với giá trị kỳ vọng dựa trên nỗ lực bỏ ra (Rogers., 1975). PMT được phát triển để giải thích tại sao lời kêu gọi sợ hãi có thể thay đổi thái độ. Lời kêu gọi sợ hãi là những thông điệp thuyết phục gây sợ hãi bằng cách mô tả hậu quả khó chịu nếu không tuân thủ các khuyến nghị (Witte., 1992, 1996). Ba khía cạnh chính trong cấu trúc này là mức độ độc hại của sự kiện (thành phần giá trị), xác suất xảy ra sự kiện không có hành động thích ứng và hiệu quả ứng phó (hai kỳ vọng) (Maddux & Rogers., 1983).

Các yếu tố này kích hoạt quy trình đánh giá nhận thức, bao gồm mức PS, PV và SE, cuối cùng kích hoạt động lực bảo vệ. Lý thuyết cho rằng thay đổi thái độ không xuất phát từ trạng thái sợ hãi mà từ mức độ động lực bảo vệ qua quá trình đánh giá nhận thức (Rogers., 1975). Nếu sự kiện không nghiêm trọng hoặc không có hành động khả thi để giảm thiểu, động cơ bảo vệ sẽ không khơi dậy, dẫn đến không thay đổi hành vi (Rogers., 1975).

Maddux & Rogers. (1983) đã bổ sung lý thuyết về năng lực bản thân, nêu rõ rằng thay đổi tâm lý xảy ra khi niềm tin của cá nhân về khả năng làm chủ tình huống của mình thay đổi (Bandura & Adams., 1977; Bandura., 1982). Tính tự tin vào SE không chỉ ảnh hưởng đáng kể đến ý định hành vi đối phó mà còn là nhân tố cảnh báo mạnh mẽ nhất về ý định hành vi, trở thành thành phần thứ tư của PMT (Maddux & Rogers., 1983).

PMT đã mở rộng để nghiên cứu các lĩnh vực khác như bảo mật thông tin. PMT đã được sử dụng để giải thích các hành vi bảo mật thông tin của người dùng phổ thông (Tsai et at., 2016; Van Bavel et at., 2019; Verkijika & De Wet., 2018) và phân tích các biện pháp bảo vệ bí mật thông tin cá nhân

trong nhiều môi trường, bao gồm hộ gia đình, tổ chức (Anderson & Agarwal., 2010; Liang & Xue, 2010; Martens et at., 2019; Thompson et al., 2017; Tu et al., 2015) và giáo dục đại học (Hina et at., 2019; Hina & Dominic., 2020; Rajab & Eydgahi., 2019).

Với mục đích của nghiên cứu này, chúng tôi áp dụng PMT bằng cách tích hợp năm biến số trung tâm của nó (PS, PV trước mối đe dọa, SE và RE, PB) làm cấu trúc bậc hai của nhận thức về an ninh mạng. CSA bao gồm PS và biện pháp bảo vệ an ninh thông tin (PS và PV), nhận thức về những gì nhân viên dự kiến sẽ làm liên quan đến bảo mật thông tin (SE và RE) và những vướng mắc trong việc thực hiện hành vi tự bảo mật (PB).

2.2. Lý thuyết về Hành vi có kế hoạch

Lý thuyết về hành vi có kế hoạch (TPB) là một mô hình giá trị kỳ vọng được áp dụng rộng rãi của các mối quan hệ thái độ - hành vi đã đạt được một số thành công nhất định trong việc dự đoán nhiều loại hành vi (Ajzen., 1985, 1991; Conner & Armitage., 1998). TPB được hình thành từ mức độ của niềm tin, thói quen hành động trong quá khứ, từ nhận thức về mức độ kiểm soát hành vi so với tự hiệu quả của bản thân, chuẩn mực đạo đức xã hội, bản sắc riêng và niềm tin tình cảm (Conner & Armitage., 1998). Những yếu tố này giúp xác định hành vi có chủ ý. TPB được coi là cải tiến của lý thuyết Hành động hợp lý (TRA), TPB đề xuất các yếu tố liên quan đến hành vi của con người dựa trên thái độ, niềm tin và ý định là những yếu tố có ảnh hưởng lớn đến sự hình thành hành vi của con người (Wu & Kuang., 2021).

Hành vi trong TPB là ý định thực hiện hành vi được đề cập; ý định càng nhiều thì khả năng thực hiện hành vi đó càng cao, TPB hành vi tổ chức và quá trình ra quyết định của con người, lý thuyết TPB đã được ứng dụng rộng rãi vào việc dự đoán và thay đổi hành vi, bao gồm cả hành vi liên quan đến việc sử dụng công nghệ (Ajzen., 2020).″TPB đã được các nhà nghiên cứu trước đây

(Liao et at., 2007; Moletsane & Tsibolane., 2020; Teo & Beng Lee., 2010; Yousuf et at., 2023; Wu & Kuang., 2021; Alanazi et at., 2022) sử dụng trong nhiều lĩnh vực để đánh giá TPB của cá nhân thông qua nhận thức, thái độ, niêm tin, ý định".

TPB bắt đầu bằng một định nghĩa rõ ràng về hành vi được quan tâm về mặt *mục tiêu,* hành *động* liên quan, *bối cảnh* xảy ra và khung thời gian (Ajzen., 2020). Nghiên cứu này mở rộng lý thuyết TPB bằng cách kiểm tra tác động của nhận thức an ninh mạng CSA (thông qua PS, RE, SE, PV, PB) đối với thái độ tuân thủ ATT, ý định tuân thủ ISPC và động lực bảo vệ thông tin IPM từ đó có ảnh hưởng như thế nào đến hành vi bảo vệ ANM (EPB) của nhân viên?

3. Lý thuyết Tuyên truyền (*Cultivation Theory - CT*)

Lý thuyết tuyên truyền (CT) là một lý thuyết truyền thông nhằm giải thích cách hành vi của người xem được hình thành bởi sự tiếp xúc với phương tiện truyền thông đại chúng (Gerbner et at., 2002). Theo CT, mọi người càng dành nhiều thời gian để tiếp nhận phương tiện truyền thông (ví dụ: TV, báo và tạp chí), thì khả năng nhận thức của mọi người về thế giới thực sẽ phù hợp với những gì phương tiện truyền thông họ tiếp nhận mô tả và truyền tải càng cao (Tang et at., 2021)

Lý thuyết Tuyên truyền còn được xem là việc tuyên truyền tới người dân thông qua phương tiện truyền thông nhằm giải thích, hướng dẫn giải quyết các vấn đề khủng hoảng của xã hội trên phương tiện thông tin đại (chúng chủ yếu là truyền hình) và ảnh hưởng đến ý kiến công chúng về các khía cạnh xã hội trong đời sống thực, người xem thực sự học được từ những phương tiện truyền thông truyền thống như phát thanh và truyền hình (Gerbner et at., 1980; Gerbner et at., 1976).

Các quốc gia đã tạo ra các hệ thống thông điệp ngày nay càng trở nên chuyên nghiệp hóa, công nghiệp hóa, tập trung hóa và chuyên môn hóa; mọi lĩnh vực xã hội đã được tuyên truyền tới người dân như: từ tôn giáo truyền thống và giáo dục chính thức sang phương tiện truyền thông đại chúng - đặc biệt là -truyền hình. Tuyên truyền thông qua phương tiện truyền thông hiện đang gắn kết các cộng đồng đa dạng, bao gồm cả những cộng đồng lớn nhóm người già trẻ và những người sống biệt lập chưa từng tham gia vào bất kỳ công chúng đại chúng nào. Truyền hình vẫn là nguồn chính của các hệ thống biểu tượng lặp đi lặp lại và nghi lễ trong một thời gian dài, nuôi dưỡng ý thức chung của những công chúng đại chúng xa xôi và không đồng nhất trong lịch sử (Gerbner et at., 1976).

Truyền hình là cơ quan trung tâm của trật tự đã được thiết lập ngày nay và như vậy chủ yếu phục vụ để duy trì, ổn định và củng cố —không phải phá hoại—các giá trị, niềm tin và hành vi thông thường. Truyền thông cho lượng khán giả lớn nhất với chi phí thấp nhất đòi hỏi những thông điệp này phải tuân theo đạo đức xã hội thông thường (Gerbner et at., 1980).

Công nghệ trực tuyến (tức là phương tiện truyền thông xã hội và trang web) đã trở thành kênh thực tế cho cả các tổ chức chính phủ và đa quốc gia như Tổ chức Y tế Thế giới (WHO) và Trung tâm Kiểm soát và Phòng ngừa Dịch bệnh Hoa Kỳ (CDC) để phổ biến thông tin và khuyến nghị cho mọi người để tránh trở thành nạn nhân của các vụ lừa đảo (Tang et at., 2021)

Lý thuyết này cho rằng tần suất sử dụng phương tiện truyền thông cao sẽ làm thay đổi nhận thức của cá nhân về thực tế xã hội, khiến nó phù hợp với mô tả của phương tiện truyền thông (Gerbner et at., 1978; Gerbner & Gross., 1976; Nabi & Riddle., 2008; Tang et at., 2021).

2.4. Không gian mạng và an ninh mạng

"Nguồn gốc của không gian mạng xuất phát từ Cơ quan Dự án Nghiên cứu Tiên tiến Quốc phòng Hoa Kỳ (DARPA) vào cuối những năm 1960, khi tiến hành thí nghiệm về mạng nội bộ nguyên mẫu gọi là "Arpanet" để kết nối các máy tính. Mục tiêu của dự án là tạo ra một phương tiện an toàn cho chỉ huy, liên lạc và kiểm soát quân sự trong một cuộc chiến tranh hạt nhân (Lantis & Bloomberg., 2018). Sự thành công của Arpanet đã dẫn đến sự ra đời của các thuật ngữ và phương pháp mới cho các tương tác trong môi trường ảo".

Đến cuối những năm 1980, các nhà nghiên cứu, khoa học và công dân bắt đầu sử dụng mạng internet để liên lạc và chia sẻ thông tin, tạo ra không gian trực tuyến gọi là không gian mạng (Carr, M. M et at., 2016). Vai trò của công nghệ trong xã hội đã được thừa nhận rộng rãi, nhưng vẫn còn hạn chế các kết quả khoa học về các khía cạnh rộng hơn như nền kinh tế kỹ thuật số, an ninh quốc gia và lợi ích xã hội.

"Không gian mạng được định nghĩa là môi trường bao gồm các thiết bị điện tử tiêu dùng, máy tính và mạng truyền thông kết nối toàn cầu. Kể từ khi Internet xuất hiện, việc sử dụng, thu nhận và tạo ra thông tin đã thay đổi đáng kể (Carr., 2016). Không gian mạng mang lại nhiều lợi ích như tiết kiệm thời gian và chi phí truy cập thông tin, thực hiện giao dịch trực tuyến và tăng cường thương mại điện tử. Ví dụ, Vương quốc Anh có tỷ lệ sử dụng thương mại điện tử cao, và Singapore dẫn đầu trong việc thực hiện chính phủ điện tử và cung cấp băng thông rộng tốc độ cao cho hầu hết các hộ gia đình (Chakravorti, B., & Chaturvedi, R. S., 2017)".

"Tuy nhiên, không gian mạng cũng gây ra các vấn đề nghiêm trọng về quyền riêng tư và bảo mật thông tin. Internet đã trở thành một hệ sinh thái rộng lớn với nhiều bên liên quan, nhưng có rất ít quy tắc hoặc hạn chế đối với hành vi của người dùng (Ronald J. Deibert; Rafal Rohozinski., 2010)".

An ninh mạng được định nghĩa là một môi trường không rủi ro được thiết lập bởi mạng lưới các thiết bị điện tử. Dù hội nhập toàn cầu đòi hỏi sử dụng nhiều công nghệ viễn thông, cuộc sống hàng ngày của người dân vẫn phải đối mặt với nguy cơ mất thông tin (Broeders, D., 2016). Sự gia tăng của các nhóm tin tặc như Anonymous và các nhóm được nhà nước bảo trợ như Dragonfly làm cho tình hình phức tạp hơn. Một mức độ bảo mật an ninh mạng nhất định cho phép người dùng tương tác trong không gian ảo mà không lo mất hoặc xâm phạm thông tin. ANM bao gồm các bước như mã hóa, tường lửa, phần mềm chống virus và hệ thống thanh toán an toàn (Bellovin, S. M., & Cheswick, W. R., 1994).

Đặc biệt, đối với các chính phủ như Singapore, Vương quốc Anh, Úc và Hoa Kỳ ANM đã trở thành nhân tố cơ bản để tối ưu hóa lợi ích của nền kinh tế kỹ thuật số và khuyến khích đổi mới. Các quốc gia phát triển đã thúc đẩy bảo mật dữ liệu để kích thích nâng cao kinh tế và tạo ra các khoản đầu tư cho kinh doanh trực tuyến. An ninh mạng không chỉ là một khái niệm mà còn là một lĩnh vực phát triển đóng góp đáng kể cho danh tiếng quốc gia. Ngược lại, các nước đang phát triển như Việt Nam còn yếu kém về công nghệ và nhận thức của công chúng về ANM vẫn còn thấp.

Để giảm thiệt hại do các mối đe dọa trực tuyến, các chính phủ cần trả lời câu hỏi quốc gia có nên kiểm soát không gian mạng trong phạm vi chủ quyền trong một kế hoạch giám sát chi tiết đa phương hay tiếp tục được chỉ dẫn bởi các bên có liên quan. Chủ các doanh nghiệp tư nhân cho rằng ANM thường được ưu tiên cho mục đích kinh doanh hơn là an ninh thực sự. Cuộc tranh luận về mật mã dữ liệu giữa các công ty công nghệ với chính phủ Hoa Kỳ đã chứng minh rằng các nhà quản lý khác nhau thì có những động thái ANM khác nhau (Collie, j., 2019).

2.5. Vấn đề bảo vệ ANM

2.5.1. Tấn công mạng và các mối đe dọa trên mạng

Trong thời đại công nghệ số, internet có tác động toàn cầu đến nhiều nền kinh tế, ảnh hưởng đến mọi khía cạnh của các hoạt động chính phủ, chính trị, cá nhân, xã hội và thương mại. Tuy nhiên, sự phát triển của công nghệ thông tin cũng mang đến những thách thức nghiêm trọng về an ninh mạng, đòi hỏi phải bảo vệ xã hội trước các mối đe dọa từ tội phạm, các cường quốc nước ngoài và khủng bố. Để đối phó với những thách thức này, cần có hành động phối hợp giữa các chính phủ và sự tham gia quốc tế, như Hiệp hội các quốc gia Đông Nam Á (ASEAN), Liên minh châu Âu (EU) và Tổ chức Hiệp ước Bắc Đại Tây Dương (NATO) (Sutherland, 2018). Vấn đề này cũng yêu cầu sửa đổi các các quy định hiện hành và ban hành các quy định mới, cũng như trang bị kiến thức mới cho công tố viên, cảnh sát và thẩm phán. Đồng thời, lực lượng vũ trang cũng cần nâng cao năng lực trong cả tấn công và phòng thủ mạng.

Trên thực tế các cuộc tấn công mạng được xem là một hiểm họa đối với nền kinh tế, xã hội và an ninh quốc gia (Sexton., 2016). "Tổ chức Hợp tác và Phát triển Kinh tế (OECD) đã phân tích 10 quốc gia vào năm 2012 và khẳng định rằng các chương trình ANM mới không chỉ để bảo vệ tổ chức mà và các cá nhân mà còn bảo vệ toàn bộ xã hội (OECD, 2012)". Tương tự như mọi chính phủ công nghiệp hóa, đảm bảo mức độ ANM phù hợp là ưu tiên của nhà nước.

Theo Tanczer et at. (2019) và Romero Moreno et at. (2020), nhiệm vụ của nhà nước là bảo vệ các quyền riêng tư của công dân khi tham trực tuyến trên không gian mạng. Các nhà quản lý đang thực hành các biện pháp để bảo vệ các cộng đồng dễ bị lạm dụng thông tin, như trẻ em, bảo mật thông tin tài chính và ngăn chặn trộm cắp danh tính. Để đưa ra các hành động đúng đắn và

giải pháp cho các mối đe dọa mạng nghiêm trọng, cần phải hiểu rõ về nền tảng của nền kinh tế kỹ thuật số và sự đổi mới mà nó mang lại.

Do nhu cầu khai thác các cơ hội và lợi thế của internet ngày càng cấp thiết trong nền kinh tế toàn cầu hóa, việc duy trì niềm tin của công chúng vào an ninh mạng là yếu tố quyết định cho sự thành công của các cơ chế xây dựng nền kinh tế kỹ thuật số của chính phủ (Carr., 2016). Các cách tiếp cận đa dạng về an ninh mạng cần được lập ra và vận dụng để hỗ trợ các cơ quan chính phủ ứng dụng linh hoạt với các thách thức về khoa học công nghệ và tăng cường bảo vệ việc kinh doanh, tài sản cá nhân và an ninh quốc gia.

2.5.2. Nhận thức về an ninh mạng

Hầu hết các tổ chức đã ban hành các chính sách và quy định liên quan đến an ninh và bảo mật. Tuy nhiên, khi nhân viên vi phạm hoặc phá vỡ các chính sách này, điều đó dẫn đến vi phạm an ninh (Puhakainen & Siponen, 2010). Hành vi sử dụng của nhân viên trở thành một điểm yếu trong cơ sở hạ tầng an ninh mạng của tổ chức (Warkentin et at., 2016). Vì vậy, hiểu được nhân tố nào ảnh hưởng đến EPB của nhân viên và giữ họ dưới sự giám sát an toàn sẽ giúp nâng cao mức độ tuân thủ chính sách bảo mật hệ thống thông tin và an ninh mạng của tổ chức (Warkentin & Willison., 2009). Chủ đề này cũng lôi cuốn sự quan tâm của các nhà quản lý và xây dựng chính sách. Để giải quyết vấn đề này, các nhân tố ảnh hưởng đến EPB của nhân viên đối với an ninh mạng cần được xác định dựa trên các lý thuyết TPB và kiểm tra bằng các bằng chứng thực hành.

2.5.3. Hành vi tuân thủ bảo mật thông tin của nhân viên

Nghiên cứu về bảo mật thông tin đã áp dụng các nguyên lý từ lý thuyết PMT để xác thực các nhân tố ảnh hưởng đến kế hoạch của người dùng trong việc chấp hành các PP bảo mật. Các biến phổ biến được xác định bao gồm chuẩn mực xã hội, SE, PB, chi phí phản hồi, PS của các biện pháp và hậu quả

bị trừng phạt, và nhận thức về sự chắc chắn sẽ bị các hậu quả trừng phạt (Han et at., 2017). Ngoài ra, các nhân tố khác ảnh hưởng đến việc tuân thủ PP bảo mật thông tin bao gồm thói quen (Vance et at., 2012), nhận thức về xác suất và mức độ nghiêm trọng của vi phạm an ninh (Herath & Rao., 2009; Vance et at., 2012). Vì vậy, kết hợp các yếu tố này giúp hiểu rõ hơn hành vi tuân thủ bảo mật thông tin của người dùng và đề xuất các biện pháp hiệu quả để nâng cao mức độ tuân thủ trong các tổ chức.

2.6. Chính sách an ninh mạng của tổ chức

Chính sách an ninh mạng của tổ chức là tuyên bố rõ vai trò và trách nhiệm của nhân viên trong việc bảo vệ tài sản công nghệ và thông tin của tổ chức (Bulgurcu et at., 2010). Chính sách này bao gồm các ý định, nguyên tắc, quy tắc và hướng dẫn mà nhân viên cần tuân theo để đảm bảo an toàn bảo mật khi tương tác với hệ thống thông tin trong quá trình làm việc (Chenet at., 2018; D'Arcy et at., 2009; Sommestad et at., 2014). Ngoài ra, chính sách cũng nêu rõ các biện pháp trừng phạt đối với hành vi vi phạm, cách sử dụng hợp lý tài nguyên máy tính và các SETA dành cho từng loại nhân viên (Sommestad et at., 2014).

Chính sách của tổ chức đóng vai trò trọng yếu trong việc làm tác động đến EPB của nhân viên và nâng cao mức độ bảo mật thông tin (Chen et at., 2018). Mặc dù vậy, một số học giả cho rằng PP ANM không ảnh hưởng nhiều đến ý định lạm dụng máy tính và hành vi lạm dụng liên quan đến sửa đổi, đánh cắp hoặc phá hủy phần mềm và dữ liệu, nhưng nhận thức về chính sách an ninh mạng thì có (D'Arcy et at., 2009; Lee & Larsen, 2009).

Kết hợp các yếu tố này giúp hiểu rõ hơn về cách chính sách an ninh mạng ảnh hưởng đến hành vi của nhân viên và đề xuất các biện pháp hiệu quả để nâng cao mức độ tuân thủ trong các tổ chức.

2.7. Nhận thức về an ninh mạng của nhân viên

Hành vi nhận thức thấp bao gồm các hành động như không tập trung hoặc bỏ qua cảnh báo bảo mật khi truy cập mạng mở miễn phí cho máy tính xách tay của công ty. Mức độ nhận thức vừa phải có thể được mô tả là sự bất cẩn trong việc sử dụng công nghệ không đúng cách (Zwilling et at., 2022). Nhận thức về an ninh mạng cấp cao là trạng thái mà nhân viên có ý thức và tích cực tuân thủ các mục tiêu bảo mật của tổ chức, như đã nêu trong nguyên tắc bảo mật của người dùng cuối (Siponen, M. T., 2000). Nó bao gồm mức độ hiểu biết của nhân viên về tầm quan trọng của an ninh mạng, trách nhiệm và hành động của họ để kiểm soát và bảo vệ dữ liệu và mạng của tổ chức (Shaw et at., 2009). Điều này cũng bao gồm sự hiểu biết về bản chất của các mối đe dọa ANM, tác hại tiềm ẩn của no và các phản ứng thích hợp để khắc phục hậu quả (Li et at., 2022).

Mức độ nhận thức ngày càng nhiều chỉ có thể xảy ra khi có sự hiểu biết toàn diện về an ninh mạng (Zwilling et at., 2022). Mặc dù có nhiều điều tra liên quan đến CSA, vẫn thiếu một cấu trúc nhất quán do các khía cạnh và trọng tâm nghiên cứu đa dạng (Hanus et at., 2018). Một số tìm hiểu đã sử dụng PMT để khái niệm hóa nhận thức về ANM thông qua đánh giá mối đe dọa và đối phó, mặc dù cấu trúc này chưa được nêu rõ ràng (Hanus et at., 2018; Herath & Rao., 2009; Lee & Larsen, 2009; Vance et at., 2012).

2.8. Truyền thông xã hội của chính phủ

Truyền thông Xã hội của Chính phủ (GSM) là sự hiện diện trực tuyến được thiết lập và giám sát bởi các cơ quan hoặc tổ chức chính phủ trên nhiều nền tảng truyền thông xã hội khác nhau (Tang et at., 2021). Tài khoản GSM giúp chính phủ tuyên truyền thông tin nhanh chóng đến người dân, thông báo về tình trạng mối đe dọa, ngăn chặn lan truyền dữ liệu sai lệch và hỗ trợ các nạn nhân bị ảnh hưởng (Guo et at., 2021).

Sự tham gia của GSM đề cập đến sự tương tác giữa các nhân viên, là người theo dõi GSM, và các tin nhắn được đăng bởi GSM (Tang et at., 2021). Các hoạt động tương tác này bao gồm xem, bình luận, chia sẻ (đăng lại), nhấp vào nút thích của bài đăng hoặc lưu bài đăng để tham khảo sau này (Guo et at., 2021).

Nhờ vào các hoạt động này, chính phủ có thể nhanh chóng tiếp cận và tương tác với công chúng, tăng cường hiệu quả trong việc truyền tải thông tin và đảm bảo an toàn thông tin.

2.9. Động cơ bảo vệ thông tin của nhân viên

Động lực bảo vệ thông tin là mức độ động lực của nhân viên trong việc thực hiện các biện pháp phòng ngừa chống lại các cuộc tấn công mạng (Vrhovec & Mihelič, 2021). Nó xuất phát từ quá trình đánh giá mối đe dọa và đối phó, hoạt động như một biến can thiệp có các đặc điểm giống như động cơ: khơi dậy, duy trì và chỉ đạo các hoạt động của nhân viên (Herath & Rao., 2009; Martens et at., 2019; Rogers., 1975). Ngoài ra, một số học giả đã trình bày lại động lực bảo vệ này như một thái độ, trong khi những người khác bỏ qua biến này và trực tiếp xem xét giá trị dự đoán của hành vi bảo vệ (Martens et at., 2019). Tuy nhiên, trong nghiên cứu này, chúng tôi giữ nguyên động lực bảo vệ như khuôn khổ ban đầu để đánh giá EPB của nhân viên.

2.10. Hành vi bảo vệ an ninh mạng của nhân viên

EPB bảo vệ ANM của nhân viên là những hành động mà nhân viên thực hiện để ứng phó đúng đắn với các rủi ro ANM (Tang et at., 2021). Các hành vi này bao gồm việc thường xuyên thay đổi mật khẩu, tuân thủ các tiêu chuẩn của tổ chức, cẩn thận trước khi nhấp vào các liên kết từ nguồn không xác định, sao lưu dữ liệu, và phần mềm, và triển khai các công cụ bảo vệ an ninh mạng (Posey et at., 2015; Tang et at., 2021). Ngược lại, các hành vi dễ gặp rủi ro bao gồm việc tiết lộ mật khẩu cá nhân, tải xuống nội dung bất hợp pháp, vi

phạm quy định bản quyền và bỏ qua các bản cập nhật phần mềm được đề xuất (Zwilling et at., 2022). Như vậy, để đảm bảo an toàn thông tin, nhân viên cần thực hiện các hành vi bảo vệ và tránh các hành vi rủi ro.

3 . Câu hỏi Nghiên Cứu

3.1. Mục tiêu nghiên cứu

Mục tiêu cuối cùng của Luận án này là kết luận tổng quan và xem xét tổng thể các mối quan hệ trung gian cũng như trực tiếp của các yếu tố trong tổ chức và xã hội có ảnh hưởng đến EPB ANM của nhân viên; góp phần làm sáng tỏ các thử nghiệm khoa học trước đây và nêu ra những khuyến nghị về giải pháp bảo đảm an toàn về ANM trong tương lai cho các nhà quản lý.

Luận án này được triển khai tổng quát thông qua triển khai mô hình điều tra của 03 lần điều tra cụ thể gồm:

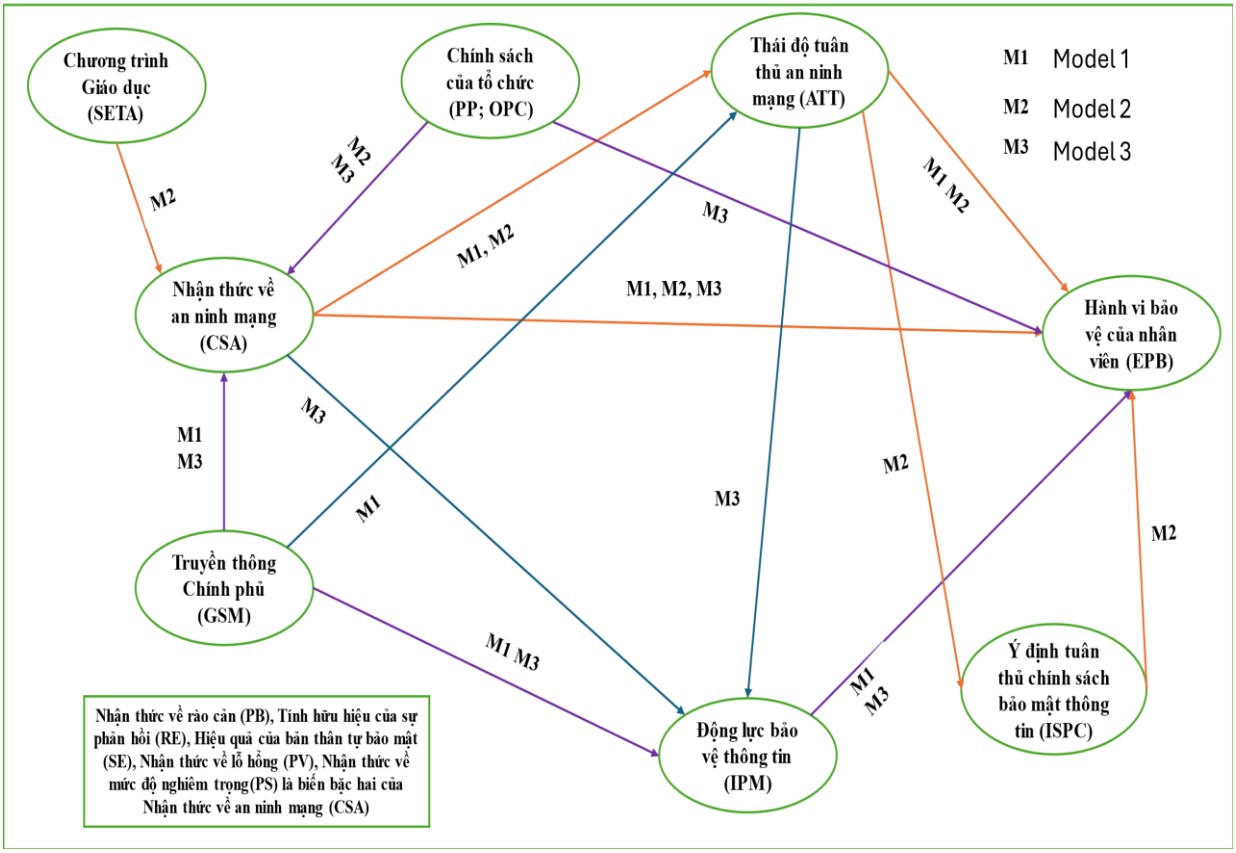
Thăm dò thứ nhất nhằm mục tiêu điều tra ảnh hưởng của sự tham gia vào mạng xã hội của chính phủ (GSM) đối với ATT an ninh mạng, IPM và EPB của nhân viên, từ đó góp phần thực hành ANM hiệu quả tại các tổ chức.

Thăm dò thứ hai tìm hiểu ảnh hưởng của CSA và ATT đối với các EPB của nhân viên. Nghiên cứu này thăm dò mối quan hệ đa dạng giữa khả năng nhận thức về các biện pháp ANM và ATT đối với việc chấp hành các biện pháp này. Ngoài ra, nó còn xem xét các nhân tố này ảnh hưởng chung đến EPB như thế nào để bảo vệ thông tin của tổ chức và tài sản.

Trong thăm dò thứ ba, nhân viên chính phủ phải chấp hành các quy tắc về quy trình bảo mật thông tin, thực hành bảo mật trực tuyến, sử dụng mạng xã hội, nghiện Internet, các mối đe dọa trực tuyến và các thói quen khác. Những hoạt động này được coi là hành vi ANM. Các tài khoản GSM ngày càng được sử dụng để giáo dục nhân viên về các rủi ro ANM. Để trợ giúp tính hiệu quả của các hoạt động an ninh mạng trong các tổ chức chính phủ, nghiên

cứu này điều tra tác động của GSM và việc tuân thủ chính sách của tổ chức đối với nhận thức, động lực và hành vi về an ninh mạng của nhân viên.

Model nghiên cứu Tổng thể của 03 nghiên cứu:



Để thực hiện được mục đích tổng quan này, luận án triển khai các mục đích cụ thể sau:

1. Kiểm tra mức độ tác động của CSA (*liên quan đến kiến thức ANM nói chung của nhân viên)* có tác động như thế nào đến EPB an ninh mạng của nhân viên.

2. Phân tích vai trò của GMS và PP, trong việc nâng cao CSA về ANM và ISPC, ATT, IPM an ninh mạng của nhân viên.

3. Xác định vai trò trung gian của Ý định tuân thủ an ninh mang, ATT và IPM có tác động như thế nào đến EPB an ninh mạng của nhân viên.

3.2. Câu hỏi nghiên cứu

Để phục vụ các mục đích chính đã đề cập ở trên, nghiên cứu này được thiết kế để trả lời các câu hỏi sau:

Câu hỏi nghiên cứu 1: Vai trò của GMS có tác động gì đến CSA và ATT an ninh mạng của nhân viên, từ đó có ảnh hưởng như thế nào tới IPM và EPB an ninh mạng của nhân viên?

Câu hỏi nghiên cứu 2: PP về an ninh mạng của tổ chức có ảnh hưởng như thế nào đến CSA của nhân viên, từ đó có ảnh hưởng như thế nào tới ISPC và ATT an ninh mạng của nhân viên; các yếu tố trên có ảnh hưởng ra sao tới EPB an ninh mạng của nhân viên?

Câu hỏi nghiên cứu 3: Truyền thông xã hội của Chính phủ, Chính sách về an ninh mạng của tổ chức có ảnh hưởng gì đến CSA về an ninh mạng của nhân viên; qua đó có ảnh hưởng gì đến Động lực bảo vệ thông tin và các EPB bảo vệ ANM của nhân viên?

4. Phương Pháp Nghiên Cứu

4.1 Bố cục của luận án

Luận án bao gồm 6 chương với những nội dung chính, như sau:

Chương I. Giới thiệu. Nội dung chương này giải thích lý do chọn chủ đề, bối cảnh điều tra, làm rõ mục đích điều tra, câu hỏi điều tra, đối tượng – phạm vi điều tra cũng như chiến thuật điều tra sẽ sử dụng đối với từng mục tiêu; diễn giải các cơ sở lý thuyết và các định nghĩa liên quan đến luận án. Bên cạnh đó, mục này cũng diễn giải những cống hiến của luận án và kết cấu của bài viết.

Chương II: "*Khám phá tác động của phương tiện GMS đối với việc tuân thủ an ninh mạng: thái độ, động lực và hành vi của nhân viên*"; Nghiên cứu này nhằm mục đích điều tra tác động của Chính phủ, thông qua các kênh truyền thông của Chính phủ (GSM) đối với ATT an ninh mạng, IPM và EPB

bảo vệ ANM của nhân viên, từ đó đóng góp ý kiến cho việc thực hành ANM thật hiệu quả tại các tổ chức.

Chương III: "*Từ nhận thức đến hành vi: Tìm hiểu việc tuân thủ an ninh mạng ở Việt Nam*". Bài viết này điều tra ảnh hưởng của CSA và ATT đối với ISPC và các EPB bảo vệ ANM của nhân viên. Nghiên cứu này tìm hiểu mối quan hệ đa dạng giữa mức độ nhận thức và các biện pháp về ANM của tổ chức và thái độ đối với việc chấp hành các biện pháp ANM này. Ngoài ra, nó còn xem xét các nhân tố này tác động chung đến EPB bảo vệ ANM của nhân viên như thế nào để bảo vệ tài sản và thông tin của tổ chức.

Chương IV: "*Làm sáng tỏ các yếu tố ảnh hưởng đến hành vi an ninh mạng của nhân viên: Một cuộc điều tra thực nghiệm trong giới công chức ở Việt Nam"*. Nhân viên chính phủ phải tuân thủ các chính sách về quy định bảo mật thông tin, thực hành bảo mật trực tuyến, sử dụng mạng xã hội, nghiện Internet, các mối đe dọa trực tuyến và các thói quen liên quan khác. Những hoạt động này được coi là hành vi an ninh mạng. Các tài khoản truyền thông xã hội của chính phủ (GSM) ngày càng được sử dụng để giáo dục nhân viên về các rủi ro an ninh mạng. Để hỗ trợ tính hiệu quả của các hoạt động an ninh mạng trong các tổ chức chính phủ, mục này điều tra tác động của GSM và việc tuân thủ PP an ninh mạng của tổ chức đối với CSA về ANM, IPM và EPB về an ninh mạng của nhân viên.

Chương V: Thảo luận các đóng góp của luận án.

Chương VI: Kết quả và khuyến nghị về Hàm ý Chính sách – diễn giải kết quả chung của các điều tra, đóng góp về mặt lý luận, đóng góp về mặt thực tế, khiếm khuyết và hướng điều tra tiếp theo.

4.2. Đối tượng nghiên cứu

Đối tượng nghiên cứu là các nhân viên hiện đang làm việc trong các cơ quan tổ chức thuộc khu vực công tại thành phố Hồ Chí Minh, Đồng Nai, Bình Dương, Nghệ An, Tây Ninh và một số tỉnh thành khác tại Việt Nam.

4.3 Thu thập dữ liệu

Cohen (1992) đã chỉ ra số mẫu dự kiến cần thu để phân tích trên phần mềm PLS Sem và quy định số mẫu tối thiểu cần thu cho model nghiên cứu tùy thuộc vào số biến của model; theo Campbell (2019) hướng dẫn việc thu mẫu, tỷ lệ phần trăm dự kiến là *d%* thì cỡ mẫu ban đầu như đã tính trước đó cần được nhân với 100/(100 - *d)* và làm tròn lên một cách thận trọng. Nếu tỷ lệ từ chối dự kiến là 67% (tức là chỉ có 1 trong 3 người trả lại bảng câu hỏi), thì số lượng bảng câu hỏi cần in là 167 x 100 / (100 - 67) = 506.06 làm tròn thành 507. Nếu chúng ta gửi 507 bảng câu hỏi và 67% không trả lại, thì chúng ta sẽ mong đợi nhận lại tổng cộng 167.

Từ tháng 10 năm 2022 đến tháng 3 năm 2023, số liệu điều tra được thu thập thông qua phân phát mẫu câu hỏi, nhắm vào các đối tượng là công chức hiện đang làm việc tại các cơ quan, tổ chức trên địa bàn các tỉnh Tp, Hồ Chí Minh, Đồng Nai, Nghệ An và một số tỉnh thành khác tại Việt Nam. Bảng câu hỏi khảo sát được phát triển trên cơ sở tham khảo các thang đo của các điều tra trước bằng tiếng Anh và sau đó được dịch sang tiếng Việt để mở rộng nhiều đối tượng trả lời hơn, những người có thể không thông thạo ngôn ngữ gốc của khảo sát. Một cuộc thử nghiệm thí điểm với 30 người trả lời, mục đích được thực hiện để kiểm tra tính đúng đắn và hợp lý của bản dịch với bối cảnh Việt Nam. Tiếp đó, những điều chỉnh cần thiết được thực hiện để nâng cao tính rõ ràng và dễ đọc của bảng câu hỏi đối với người được hỏi.

Cuối cùng, một cuộc khảo sát đại trà tiến hành với 1450 mẫu câu hỏi được phân phát (thông qua 03 lần phát mẫu cho 03 mô hình nghiên cứu), thu về 1200 mẫu, sử dụng 976 mẫu dùng để phân tích và đo lường; *lần thứ nhất*,

phát mẫu cho mô hình nghiên cứu thứ nhất là 500 mẫu phát đi, thu về 380 mẫu, sử dụng 323 mẫu để đo lường và phân tích; *lần thứ hai*, phát mẫu cho mô hình nghiên cứu thứ hai là 450 mẫu phát đi, thu về 400 mẫu, sử dụng 323 mẫu để đo lường và phân tích; *lần thứ ba*, phát mẫu cho mô hình nghiên cứu thứ ba là 500 mẫu phát đi, thu về 420 mẫu, sử dụng 330 mẫu để đo lường và phân tích.

Các câu hỏi được trả lời được coi là không phù hợp cho nghiên cứu có thể là do các câu trả lời đồng nhất cho tất cả các câu hỏi (ví dụ: tất cả 1 hoặc tất cả 7) và việc hoàn thành khảo sát trong vòng chưa đầy hai phút (Collier & Sherrell, 2009).

4.4 Đo lường

Tất cả các câu hỏi được đánh giá bằng thang đo Likert 7 điểm, từ 1 (rất không đồng ý) đến 7 (rất đồng ý). Bảng câu hỏi được sửa đổi từ các điều tra cũ với những sửa đổi nhỏ hoặc lớn. Phần đầu tiên của cuộc khảo sát bao gồm thông tin nhân khẩu học như giới tính, tuổi tác, trình độ học vấn, thời gian làm việc và quy mô tổ chức . Phần thứ hai bao gồm các công trình và các hạng mục đo lường tương ứng của chúng. Các chỉ số đánh giá chính sách của tổ chức và mức độ nghiêm trọng được nhận thấy được lấy từ Hina et at. (2019). Các biện pháp đánh giá nhận thức về lỗ hổng và hiệu quả ứng phó được rút ra từ các nghiên cứu trước (Hina et at.,,2019; Li et at., 2019; Wong et at., 2022). Hiệu quả bản thân được đo lường bằng cách sử dụng các thang đo phỏng theo Hina et at. (2019) và Li et at. (2022). Các thang đo truyền thông xã hội của chính phủ được chọn quảng cáo từ Tang et at. (2021). Động lực bảo vệ thông tin được đánh giá dựa trên thang đo của Ma (2022) và Posey et at. (2015). Hành vi bảo vệ của người lao động được phỏng theo Bulgurcu et at. (2010) và Wong et at. (2022); Các hạng mục đo lường được trình bày chi tiết và cụ thể theo kết cấu của từng nghiên cứu.

4.5 Phương pháp nghiên cứu

Trong nghiên cứu này, mô hình phương trình cấu trúc bình phương nhỏ nhất từng phần (PLS-SEM) được áp dụng để phân tích dữ liệu thực nghiệm thu thập được và đánh giá mô hình nghiên cứu. PLS-SEM là một phương pháp dựa trên phương sai để đánh giá các cấu trúc mô hình từng phần thông qua việc tích hợp phân tích các thành phần nguyên tắc với hồi quy bình phương nhỏ nhất thông thường (Hair et at., 2020). PLS-SEM đã được sử dụng rộng rãi trong một số lĩnh vực bao gồm hệ thống thông tin quản lý (Ringle et at., 2013) và hành vi an ninh mạng (Alanazi et at., 2022; Wong et at., 2022). PLS-SEM phù hợp tốt với các mục tiêu nghiên cứu của chúng tôi: *thứ nhất*, nó có thể kiểm tra khung lý thuyết từ quan điểm dự đoán; *thứ hai*, nó hỗ trợ mô hình cấu trúc phức tạp và bao gồm nhiều cấu trúc, chỉ báo, thành phần phụ thuộc và mối quan hệ mô hình; *thứ ba*, nó giúp nâng cao khả năng hiểu khi khám phá phần mở rộng lý thuyết của các lý thuyết đã được thiết lập; *thứ tư,* nó cung cấp khả năng thống kê tuyệt vời mà không cần cỡ mẫu lớn và giải quyết hiệu quả các vấn đề như giá trị bị thiếu, thiếu tính chuẩn, đa cộng tuyến (Hair et at., 2019; Hair et at., 2020; Henseler et at., 2016). Ứng dụng Smart PLS 4.0 đã được sử dụng để phân tích.

PLS-SEM cung cấp các ước tính chính xác hơn với kích thước mẫu nhỏ và do đó nên áp dụng nó trong những trường hợp như vậy (Hair & Sarstedt., 2019). PLS-SEM có nhiều khả năng dẫn đến sự hội tụ mô hình khi nghiên cứu một số lượng lớn các biến được quan sát và/hoặc biến tiềm ẩn, và nó phù hợp hơn -khi các mô hình phức tạp (Hair et al., 2019; Hair et at., 2018). PLS-SEM nên được chọn khi dự đoán là trọng tâm chính của nghiên cứu (Shmueli et at., 2016, 2019). PLS-SEM có thể dễ dàng được sử dụng với các mô hình đo lường hình thành, dữ liệu phi số liệu (ví dụ: thứ tự và danh nghĩa) và các bộ điều tiết liên tục (Hair et al., 2020).

4.6. Giới hạn điều tra

Giới hạn điều tra của luận án là: cán bộ công chức thường xuyên làm việc trên máy tính hiện đang làm việc trong khu vực công tại Việt Nam (*đối tượng phát mẫu gồm: cán bộ Công an hiện đang công tác tại các Cục nghiệp vụ thuộc Bộ Công an, các Giảng viên thuộc các trường Công An nhân dân, cán bộ thuộc sở ban ngành thuộc khối hành chính sự nghiệp tại thành phố Hồ Chí Minh, Đồng Nai, Bình Dương, Nghệ An, Hà Nội…., một số đơn vị bồ đội trực thuộc Bộ Quốc phòng và thảo luận nhóm cùng một số chuyên gia an ninh mạng đến từ các trường trong Công An nhân dân, trường Đại học Quốc tế và trưởng bộ phận phụ trách công nghệ thông tin tại các ngân hàng thương mại*.

Chương II. Khám phá ảnh hưởng của phương tiện truyền thông xã hội của chính phủ đối với việc tuân thủ an ninh mạng: thái độ, động lực và hành vi của nhân viên

Chương này được trình bày từ kết quả bài báo thứ nhất đã được đăng: Tran, D. Van, Nguyen, P. Van, Nguyen, A. T. C., Vrontis, D., & Dinh, P. U. (2024). Exploring the influence of government social media on cybersecurity compliance: employee attitudes, motivation and behaviors. *Journal of Asia Business Studies, 18*(1), 204-223. https://doi.org/10.1108/JABS-09-2023-0343. Scopus Q1.

Nghiên cứu này nhằm mục đích điều tra tác động của GSM khi tham gia vào mạng xã hội của chính phủ đối với ATT, IPM và EPB bảo vệ của nhân viên, từ đó đóng góp vào việc nâng cao hiệu quả ANM tại các tổ chức. Để hoàn thành mục tiêu này, luận án sử dụng phương pháp phân tích định lượng với dữ liệu khảo sát được thực hiện tại các thành phố và tỉnh lớn ở Việt Nam. Kết quả là, 323 câu trả lời đã được thu thập và phân tích PLS-SEM. Kết quả phân tích cho thấy sự tham gia vào GSM có ảnh hưởng tích cực đến thái độ tuân thủ an ninh mạng của nhân viên. Hơn nữa, nhận thức về lỗ hổng trước mối đe dọa và hiệu quả ứng phó cũng góp phần tạo nên thái độ tuân thủ tích cực. Tuy nhiên, tính tự tin vào khả năng của bản thân lại có tác động tiêu cực đến ATT. ATT an ninh mạng giải thích đáng kể IPM, từ đó ảnh hưởng đến hành vi bảo vệ của nhân viên. Tuy nhiên, mối quan hệ giữa thái độ tuân thủ và hành vi bảo vệ lại yếu hơn so với các nghiên cứu trước đây. Đáng chú ý, mặc dù các nghiên cứu gần đây đã khám phá các thực tế bảo mật thông tin trong bối cảnh doanh nghiệp và gia đình, ảnh hưởng của GSM đối với EPB an ninh mạng của cá nhân nhận được sự quan tâm còn hạn chế. Do đó, điều tra này góp phần vào nền tảng lý luận hiện có bằng cách điều tra ảnh hưởng của GSM đối với các EPB an ninh mạng, đồng thời mở rộng lý thuyết PMT và lý thuyết CT.

1. Giới thiệu

Sự phổ biến của các cuộc tấn công mạng thù địch ngày càng gia tăng do sự phát triển nhanh chóng của công nghệ kỹ thuật số, điều này làm tăng nhu cầu chống lại các mối đe dọa an ninh mạng (Harris & Patten., 2014; He, 2012, 2013; Peréz-Morón & Cantillo-Orozco, 2022). Một số cuộc tấn công mạng phổ biến đã sử dụng phần mềm độc hại, một loại phần mềm độc hại để xâm nhập vào mạng, cho phép những kẻ phát tán phần mềm này tống tiền chủ sở hữu mạng đó hoặc làm hỏng mạng đó. Một phương pháp phổ biến khác là lừa đảo, trong đó các tin nhắn điện tử lừa đảo được gửi đến những người dùng vô tình để lấy thông tin nhạy cảm mà người gửi không có quyền. Phương pháp thứ ba là tấn công trung gian, trong đó dữ liệu giao dịch được trao đổi giữa hai bên thông qua mạng công cộng bị bên thứ ba chặn và đánh cắp. Các biện pháp bảo mật thông tin mạnh mẽ phải được sử dụng để bảo vệ dữ liệu quan trọng của công ty được lưu trữ trong các mạng này (Zhang et at., 2017). Do những tiến bộ công nghệ, các quốc gia và tổ chức quốc tế ngày càng dựa vào các nền tảng truyền thông xã hội để chia sẻ thông tin và đưa ra lời khuyên về cách ngăn chặn các sự kiện an ninh mạng lớn này (Beaunoyer et at., 2020; Chen et al., 2020; Farooq et al., 2020).

Các nghiên cứu trước đây đã kết luận rằng mạng xã hội có thể đóng vai trò quan trọng trong việc phổ biến các cảnh báo (Beaunoyer et at., 2020; Chen et at., 2020; Farooq et at., 2020; Guo et at., 2021). Tuy nhiên, tài liệu về truyền thông xã hội của chính phủ (GSM) - tức là việc chính phủ sử dụng truyền thông xã hội - vẫn còn ở giai đoạn sơ khai. Phần lớn nghiên cứu hiện nay tập trung vào việc xác định lý do tại sao mọi người sử dụng GSM (Chen et at., 2020; Guo et at., 2021; Nguyen et at., 2023) hoặc chiến lược nhắn tin được sử dụng trong GSM (Chatterjee et at., 2021; Lee & Cho, 2018; Li et at., 2022). Đặc biệt, một số nghiên cứu thực nghiệm khám phá tác động của sự tham gia vào GSM đối với kết quả hành vi. Ngoài ra, nghiên cứu trước đây chủ yếu dựa

vào dữ liệu thu được từ người dùng Internet và các công ty truyền thông xã hội tư nhân trên các nền tảng mạng xã hội khác nhau, thay vì tìm nguồn cung cấp thông tin trực tiếp từ GSM chính thức đến người dùng cá nhân.

Ngoài ra, nhiều nhà nghiên cứu đã chỉ ra rằng cả hai tổ chức (Anderson, & Agarwal, 2010; Johnston et at., 2019; Johnston & Warkentin., 2010; Warkentin et at., 2016) và hộ gia đình (Liang & Xue, 2010; Martens et at., 2019; Tu et at., 2015) thực hiện các biện pháp bảo mật thông tin cụ thể. Tuy nhiên, thật khó để xác định tác động của GSM đối với những hành vi bảo vệ này. Hành vi bảo mật thông tin đã nhận được rất nhiều quan tâm nghiên cứu, nhưng kết quả không nhất quán, một phần vì các nghiên cứu không tính đến thái độ và động lực (Ma., 2022). Vì vậy, để đảm bảo rằng các biện pháp bảo mật được thực hiện để bảo vệ các hệ thống khác nhau là toàn diện, chúng tôi kiểm tra ảnh hưởng của thái độ và động lực của mọi người đối với hoạt động an ninh mạng của họ.

Do khả năng truy cập Internet ngày càng tăng, mức độ phức tạp và tần suất của các cuộc tấn công mạng đã leo thang rõ rệt. Sự tồn tại của loại hoạt động có hại này đã gây ra những tác động tiêu cực đáng kể và lan rộng, ảnh hưởng đến các công ty, toàn bộ ngành công nghiệp và thậm chí cả chính phủ các quốc gia. Do đó, các chính phủ đã thực hiện các biện pháp cụ thể nhằm bảo vệ các mạng liên quan đến an ninh quốc gia. Mục tiêu là tăng cường khung pháp lý liên quan đến an ninh thông tin mạng để đảm bảo bảo vệ mạnh mẽ các thông tin quốc phòng quan trọng. Để làm như vậy, các chính phủ phải ưu tiên đánh giá khả năng và kinh nghiệm vận hành của những người giám sát mạng lưới. Hơn nữa, việc triển khai khung pháp lý toàn diện là rất quan trọng để quản lý hiệu quả an ninh thông tin mạng, chủ yếu nhằm giảm thiểu rủi ro và chống lại các mối hiểm họa trên không gian mạng. Ngày 12/6/2018, Quốc hội Việt Nam đã thông qua Luật An ninh mạng, có hiệu lực từ ngày 1/1/2019. Luật này điều chỉnh các hoạt động nhằm bảo đảm trật tự, an toàn xã hội trên

không gian mạng và trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan. Tuy nhiên, cần phải nghiên cứu sâu hơn, hoàn thiện quy định này để đảm bảo an toàn cho các cá nhân, tổ chức khi sử dụng Internet và giao dịch trực tuyến.

Để giải quyết lỗ hổng trong tài liệu, nghiên cứu của chúng tôi sử dụng lý thuyết Động lực bảo vệ (PMT) (Johnston & Warkentin., 2010) và lý thuyết Tuyên truyền (Gerbner et at., 2009; Gerbner & Gross., 1976; Hermann et at., 2020). Chúng tôi xây dựng dựa trên những lý thuyết này bằng cách kết hợp thái độ tuân thủ và động lực bảo vệ làm yếu tố tiền thân, để có được kiến thức toàn diện về động cơ thúc đẩy EPB. Chủ đề này dựa trên các câu trả lời cho các câu hỏi nghiên cứu sau:

RQ1. Sự tham gia vào GSM của nhân viên ảnh hưởng như thế nào đến thái độ của họ đối với việc tuân thủ các biện pháp an ninh mạng?

RQ2. Mối quan hệ giữa thái độ của những nhân viên này đối với sự tuân thủ, động cơ bảo vệ và hành vi bảo vệ là gì?

Những phát hiện của nghiên cứu này đóng góp đáng kể cho những người thực hành bằng cách làm sáng tỏ mối quan hệ giữa sự tham gia vào GSM, thái độ tuân thủ, động cơ bảo vệ và hành vi bảo vệ. Nghiên cứu của chúng tôi cung cấp cho các chuyên gia những hiểu biết có giá trị về tác động có thể có của mạng xã hội trong việc tạo điều kiện thuận lợi cho việc phân phối thông tin nhằm giải quyết và giảm bớt những lo ngại về an ninh mạng. Nghiên cứu của chúng tôi nhấn mạnh hơn nữa tầm quan trọng của việc tự -vệ đối với người dùng cá nhân. Hơn nữa, các cơ quan chính phủ và các doanh nghiệp khác nên triển khai các chương trình đào tạo về bảo mật thông tin đã được tùy chỉnh để giải quyết các mối lo ngại về bảo mật. Mục tiêu chính của các chương trình này là nâng cao năng lực của các cá nhân, bao gồm cả nhân sự, trong việc đánh giá thành thạo các mối nguy hiểm an ninh tiềm ẩn và thực hiện các biện pháp đối phó phù hợp. Việc chứng thực một số hoạt động quan

trọng là rất quan trọng, bao gồm việc thực hiện các chiến dịch thường xuyên được thiết kế để giáo dục nhân viên về nhu cầu giảm thiểu dấu chân trực tuyến của họ, thúc đẩy sự an toàn của nhân viên và phát hiện các mối đe dọa nội bộ.

2. Cơ sở lý thuyết

2.1 Lý thuyết Động cơ bảo vệ

PMT là lý thuyết được sử dụng thường xuyên nhất trong các nghiên cứu về an ninh hành vi (Wall & Warkentin. 2019), vì nó giải thích cách mọi người diễn giải mối nguy hiểm và quyết định sử dụng biện pháp phòng vệ nào trong các hành vi bảo vệ. Theo PMT, hai quá trình làm nền tảng cho cách mọi người phản ứng với rủi ro và tự bảo vệ mình: đánh giá mối đe dọa và đánh giá đối phó. Mối đe dọa được đánh giá bằng phương pháp đánh giá mối đe dọa, được chia nhỏ thành đánh giá mức độ nghiêm trọng và nhận thức về lỗ hổng (PV) (Witte et at., 2010). Tuy nhiên, một số điều tra trước đây nhấn mạnh sự chồng chéo giữa mức độ nghiêm trọng và tính nhạy cảm được nhận thức (Ameen et at., 2021; Ifinedo., 2012). Để phù hợp với những nghiên cứu này, chúng tôi kết hợp PV vào mô hình nghiên cứu khi dự đoán PMT trong quá trình đánh giá mối đe dọa.

Trong đánh giá đối phó, mọi người đánh giá các phản ứng tiềm ẩn đối với các mối nguy hiểm đồng thời với việc đánh giá các rủi ro. Quá trình này đánh giá xu hướng của một người trong việc thực hiện các biện pháp bảo vệ cần thiết để giảm thiểu mối đe dọa, có thể được chia nhỏ thành hiệu quả ứng phó (RE), tính tự tin vào năng lực bản thân (SE) và chi phí ứng phó (Johnston & Warkentin., 2010; Witte et at., 2010). Tiếp theo Martens et at. (2019), nghiên cứu này không xem xét chi phí phản hồi vì nó không rõ ràng và việc đo lường nó là một thách thức (Warkentin et at., 2011).

2.2 Lý thuyết Tuyên truyền (*Cultivation Theory - CT*)

Lý thuyết Tuyên truyền là một lý thuyết về giao tiếp được George Gerbner và các đồng nghiệp của ông đưa ra vào những năm 1970 để giải thích những thay đổi trong hành vi của người xem do tiếp xúc với các phương tiện thông tin đại chúng (Gerbner et at., 2009; Hermann et at., 2020). Tuyên truyền được định nghĩa là nhận thức của người xem về thực tế xã hội do tiếp xúc với thông tin qua mạng xã hội (Gerbner et at., 2009). Nói cách khác, việc tiếp xúc thường xuyên trên mạng xã hội giúp mọi người phát triển và duy trì những niềm tin riêng biệt (Cheng et at., 2016). Hiệu ứng lan tỏa của mạng xã hội có thể thay đổi cách người xem hiểu thế giới, tùy thuộc vào thông tin được trình bày trên mạng xã hội chứ không phải trên thực tế (Hermann et at., 2020). Phương tiện truyền thông xã hội sử dụng hai quá trình nhận thức để tác động đến dư luận trong giai đoạn trau dồi: lồng ghép và cộng hưởng (Tang et at., 2021).

Khi quan điểm của các cá nhân phù hợp với nội dung họ thu được từ các nền tảng truyền thông xã hội, sự cộng hưởng sẽ được tăng cường, củng cố hiệu quả tuyên truyền.

2.3 Truyền thông xã hội của chính phủ

Việc sử dụng phương tiện truyền thông xã hội trong chính phủ là một trong những xu hướng chính trong nghiên cứu và thực hành chính phủ điện tử (tức là số hóa trong các chức năng của chính phủ) trong những năm gần đây (Criado et al., 2013). Tài khoản GSM chính thức, theo định nghĩa của nghiên cứu này, là một hồ sơ công khai trực tuyến được cơ quan chính phủ tạo và duy trì trên mạng xã hội để phổ biến thông tin và thu thập phản hồi từ người dùng (Medaglia & Zhu., 2017). Sự tương tác hoặc tham gia GSM được định nghĩa là sự tương tác với các tin nhắn (ví dụ: đọc, bình luận hoặc phản hồi và chia

sẻ bài đăng) được đăng bởi tài khoản GSM bởi người dùng hoặc người theo dõi các tài khoản đó (Guo et at., 2021).

Phương tiện truyền thông xã hội được đặc trưng bởi khả năng giảm thiểu hoặc loại bỏ các rào cản giao tiếp giữa các cá nhân (hoặc giữa các cá nhân và đại diện tổ chức) và tạo môi trường thuận lợi cho sự giao tiếp giữa công dân với chính phủ của họ. Trong tài liệu, khả năng này được thừa nhận là một phương tiện công nghệ trọng yếu mà các chính phủ vận dụng để truyền đạt các cảnh báo và các loại thông tin khác tới công chúng. Hơn nữa, tác dụng tuyên truyền của nó giúp nâng cao nhận thức và kiến thức về tình huống của các cá nhân, củng cố hơn nữa tiềm năng của nó trong việc phát đi những thông tin quan trọng (Beaunoyer et at., 2020; Chen et at., 2020; Farooq et at., 2020; Guo et at., 2021). Tuy nhiên, một số điều tra thực nghiệm đã xem xét ảnh hưởng của việc tham gia vào GSM đối với hành vi của người dân.

2.4 Thái độ, động cơ và hành vi bảo mật thông tin

Trong bối cảnh bảo mật thông tin, chúng tôi định nghĩa EPB là những hành động họ thực hiện để tránh các vấn đề về bảo mật thông tin (Martens et at., 2019; Tu et at., 2015). Hơn nữa, thái độ tuân thủ an ninh mạng (ATT) được định nghĩa là quan điểm tích cực về việc tuân thủ các chính sách bảo mật thông tin (Wong et at., 2022). Nhiều nghiên cứu tập trung vào cách đảm bảo EPB và ATT tuân thủ an ninh mạng (Anderson & Agarwal, 2010; Ifinedo., 2012; Siponen et at., 2014) và những người khác kiểm tra xem liệu một nhân viên có ý định vi phạm chính sách bảo mật thông tin hay không (Siponen & Vance., 2010) hoặc lạm dụng hệ thống thông tin. Vẫn còn những nghiên cứu trước đây tập trung vào bối cảnh cá nhân (Liang & Xue, 2010; Martens et at., 2019; Tu et at., 2015) và bối cảnh tổ chức (Johnston & Warkentin., 2010; Nair et at., 2019; Warkentin et at., 2016). Tuy nhiên, thái độ tuân thủ, động cơ bảo vệ và sự tham gia vào các EPB của nhân viên lại ít được chú ý.

3. Phát triển giả thuyết

3.1 Phương tiện truyền thông xã hội của chính phủ, nhận thức về tính dễ bị tổn thương, tính tự hiệu quả và hiệu quả ứng phó

PV là ước tính của mọi người về khả năng bị tổn hại hoặc quan điểm về khả năng họ trở thành nạn nhân của một mối đe dọa cụ thể (Johnston & Warkentin., 2010; Witte et, al., 2010). SE là sự tự đánh giá của một người về khả năng thực hiện hành vi bảo vệ hoặc liệu một người có kiến thức, khả năng và nguồn lực cần thiết để thực hiện nhiệm vụ một cách có trách nhiệm hay không (Maddux & Rogers, 1983). RE có nghĩa là mức độ tin tưởng của mọi người rằng giải pháp được đề xuất sẽ giảm thiểu thành công mức độ đe dọa đối với họ (Tang et at., 2021).

Nghiên cứu trước đây về lý thuyết CT đã chỉ ra rằng việc các cá nhân sử dụng mạng xã hội có ảnh hưởng đáng kể đến thái độ và nhận thức của họ (Albashrawi et at., 2022; Gerbner et at., 2009; Gerbner & Gross., 1976; Hermann et at., 2020). Những người dành nhiều thời gian hơn trên mạng xã hội có nhiều khả năng nhận thức rằng thế giới thực giống với những gì họ thấy và nghe trên mạng xã hội. Tác động của việc áp dụng mạng xã hội đối với quá trình đánh giá mối đe dọa đã được ghi chép rõ ràng (Intravia et at., 2017; Kim & Hawkins., 2020; Shah et at., 2020). Nghiên cứu trước đây chỉ ra rằng, bất kể phương tiện truyền thông nào, việc tiếp xúc nhiều hơn với thông tin về thảm họa hoặc tội phạm sẽ khiến các cá nhân trải qua mức độ lo lắng cao hơn. Điều này có thể là do nhận thức rằng bản thân những cá nhân này, gia đình họ hoặc những người khác có thể trải qua những sự kiện được mô tả trên các phương tiện truyền thông (Intravia et at., 2017; Kim & Hawkins., 2020; Shah et at., 2020). Nghiên cứu này kiểm tra quan điểm cho rằng việc tham gia GSM có thể được xem là một dạng hành động sử dụng mạng xã hội. Chúng tôi phát triển giả thuyết rằng những người tham gia vào các hoạt động như đọc, bình

luận và chia sẻ thông tin bảo mật bắt nguồn từ GSM có xu hướng có thái độ tuân thủ hơn và có ý thức hơn về PV. Hai giả thuyết đầu tiên được tuyên bố như sau:

H1. Sự tham gia vào GSM có liên quan tích cực đến thái độ tuân thủ ATT về an ninh mạng.

H2. Sự tham gia vào GSM có mối liên hệ tích cực với PV.

Ngoài việc gây ra nỗi sợ hãi hoặc cảm giác bị đe dọa giữa các cá nhân, nền tảng truyền thông xã hội còn là một phương tiện giáo dục người dùng về cách nâng cao khả năng chuẩn bị cho những nguy hiểm, chẳng hạn như thiên tai (Farooq et at., 2020). Theo lý thuyết Tuyên truyền, mọi người có thể đánh giá sự thành công của việc sử dụng các phản ứng phòng thủ bằng cách sử dụng kiến thức mà họ tích lũy được từ GSM làm nền tảng, từ đó làm tăng RE của họ (Tang et at., 2021; Tu et at., 2015). Hơn nữa, mọi người có thể cải thiện SE của mình bằng cách tìm hiểu và nhận thông tin về đánh giá mối đe dọa trên mạng xã hội (Kim & Hawkins., 2020; Tu et at., 2015). Mọi người có nhiều khả năng tự tin hơn khi sử dụng một số biện pháp nhất định khi họ hiểu biết nhiều hơn về các biện pháp đối phó khả thi trước các mối nguy hiểm (Tang et at., 2021; Tu et at., 2015). Do đó, chúng tôi đưa ra giả thuyết rằng niềm tin của nhân viên vào khả năng giảm thiểu rủi ro của họ có thể sẽ gắn kết với GSM. Do đó, các giả thuyết tiếp theo được đề xuất:

H3. Sự tham gia vào GSM có mối liên hệ tích cực với SE.

H4. Sự tham gia vào GSM có mối liên hệ tích cực với tính hữu hiệu của sự phản hồi RE.

3.2 Nhận thức về tính dễ bị tổn thương, tính tự hiệu quả và hiệu quả ứng phó

Mức độ quen thuộc của nhân viên với những mối nguy hiểm tiềm ẩn và khả năng quản lý chúng có khả năng ảnh hưởng đến hành vi của họ thông qua việc hình thành niềm tin về hành vi, quy chuẩn hoặc kiểm soát trong bối cảnh an ninh (Bulgurcu et at., 2010). Theo PMT, những người tin rằng họ dễ bị tổn thương trước các mối đe dọa thường có thái độ tuân thủ đối với vấn đề bảo mật thông tin (Hina et at., 2019). Nghiên cứu trước đây chỉ ra rằng những người có kiến thức về mối nguy hiểm tiềm ẩn có nhiều khả năng thực hiện các biện pháp phòng ngừa để tránh trở thành nạn nhân của mối đe dọa đó (Johnston & Warkentin., 2010). Do đó, thái độ tuân thủ của họ bị ảnh hưởng tích cực (Anderson & Agarwal., 2010; Wong et at., 2022). Do đó, chúng tôi đưa ra giả thuyết rằng những nhân viên có cảm giác dễ bị tổn thương cao hơn sẽ thể hiện thái độ ủng hộ hơn trong việc dành nhiều nỗ lực hơn nữa để đảm bảo an toàn cho nhiệm vụ. Do đó, giả thuyết tiếp theo được đặt ra:

H5. PV có mối liên hệ tích cực với ATT.

Theo PMT, phản ứng đánh giá đối phó của nhân viên phụ thuộc vào niềm tin của họ vào năng lực thực hiện hoàn thành nhiệm vụ cũng như kỳ vọng của họ về hiệu quả của họ (Sharma et at., 2020). SE được áp dụng trong điều tra trước đây để lý giải thái độ liên quan đến máy tính của mọi người (Crossler et at., 2013; Johnson & Marakas., 2000; Ma., 2022; Wong et at., 2022). Tuy nhiên, những điều tra thực nghiệm này có kết quả mâu thuẫn với nhau. Đặc biệt, SE và ATT có mối liên hệ tích cực (Anderson, C.L. and Agarwal, R., 2010; Johnston & Warkentin., 2010), nhưng các điều tra khác cho thấy các nhân tố này có tác động khác đến nhau (Hooper & Blunt, 2020; Moody et at., 2018). Trong chủ đề này, chúng tôi tìm hiểu sâu hơn về mối liên hệ giữa SE và sự tuân thủ, đề xuất giả thuyết sau:

H6. Hiệu quả của bản thân tự bảo mật SE được liên kết với thái độ tuân thủ an ninh mạng ATT.

Dựa trên PMT, điều tra trước đây đã nhận định rằng các cá nhân có thể chọn không tham gia vào các hành động bảo vệ nếu họ nhận thấy một biện pháp bảo mật vừa đơn giản để cài đặt vừa không hiệu quả (Hanus & Wu., 2016; Johnston & Warkentin., 2010; Wong et at., 2022). Nói cách khác, RE ảnh hưởng tích cực đến ATT của mọi người đối với việc áp dụng các EPB an ninh thông tin cá nhân đã đề xuất. Các nhà điều tra khác cho rằng mối liên hệ này không đáng kể (Siponen et at., 2014). Mặc dù, những kết quả không đồng nhất, chủ đề này giả định rằng nhân viên có ATT cực hơn đối với phản hồi được đề xuất nếu họ tin vào hiệu quả của nó. Do đó, đề xuất giả thuyết sau:

H7. RE có mối liên hệ tích cực với ATT.

3.3 Thái độ tuân thủ, động cơ bảo vệ và hành vi bảo vệ

Từ góc độ PMT, thái độ ảnh hưởng đến ý định tuân theo các quy định bảo mật của nhân viên và có mối tương quan tích cực với việc tuân thủ các chính sách bảo mật thông tin của tổ chức (Siponen et at., 2014). Ma. (2022) cũng nhận thấy rằng thái độ tích cực đối với việc bảo vệ an ninh thông tin sẽ tác động tích cực đến IPM của nhân viên. Nhiều nghiên cứu trước đây có kết quả tương tự (Ameen et al., 2021; Hina et at., 2019; Ma. 2022; Martens et at., 2019; Safa et at., 2015; Wu, 2020). Phù hợp với nghiên cứu trước đây, chúng tôi tin rằng những nhân viên có thái độ tích cực đối với việc bảo vệ tài sản thông tin của họ và của tổ chức họ sẽ có động lực bảo vệ thông tin (IPM) lớn hơn và hành vi bảo vệ nhiều hơn. Do đó, các giả thuyết sau được đề xuất:

H8. Thái độ tuân thủ an ninh mạng ATT có liên quan đến EPB bảo vệ ANM của nhân viên.

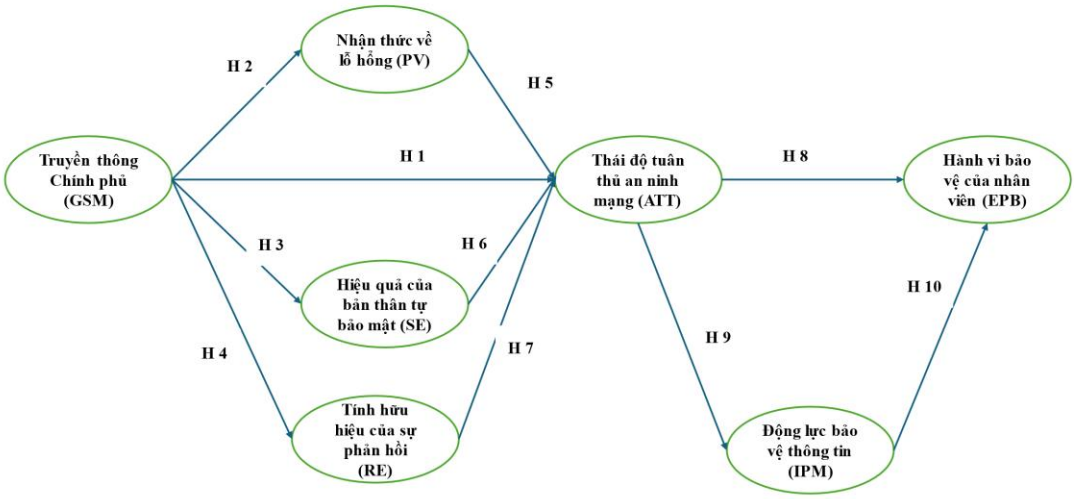
H9. Thái độ tuân thủ an ninh mạng ATT có liên quan tích cực với Động lực bảo vệ thông tin IPM.

PMT nên được mở rộng để dự đoán hành vi vì mục tiêu của nghiên cứu bảo mật thông tin là cải thiện EPB chứ không phải là tăng cường ý định bảo vệ (Floyd et at., 2006). Phù hợp với quan điểm này, Liang and Xue (2010) tích hợp EPB thực tế vào khung thử nghiệm và khám phá mối tương quan tích cực giữa những người thể hiện động lực cao hơn để tham gia bảo vệ thông tin và xu hướng tham gia vào các biện pháp nhằm ngăn ngừa sự cố an ninh thông tin cao hơn. Các bài báo khác xác nhận những phát hiện tương tự (Lebek et at., 2014; Siponen et at., 2014; Warkentin et at., 2016). Trong nghiên cứu này, chúng tôi tin rằng EPB phụ thuộc vào động cơ bảo vệ an ninh thông tin IPM. Do đó, đề xuất giả thuyết sau:

H10. Động lực bảo vệ thông tin IPM có mối liên hệ tích cực với EPB bảo vệ ANM.

Như đã thảo luận trước đó, mối quan hệ giữa các cấu trúc được đề xuất cho mô hình khái niệm này được thể hiện trong Hình 1. Mô hình nghiên cứu bao gồm sự tham gia vào GSM, PV, SE, RE, ATT tuân thủ an ninh mạng, IPM và EPB. Mô hình khái niệm này đánh giá mối quan hệ giữa các cấu trúc này và dựa trên mười giả thuyết của chúng tôi.

Hình 2.1: Mô hình nghiên cứu đề xuất



4. Phương pháp nghiên cứu

4.1 Thang đo

Công cụ khảo sát trong nghiên cứu này được tạo ra bằng cách sử dụng các tài liệu có sẵn. Tất cả các câu hỏi trong cuộc khảo sát này được chấm điểm theo thang đo Likert bảy điểm, từ 1 = "hoàn toàn không đồng ý" đến 7 = "hoàn toàn đồng ý". Tất cả các thang đo được điều chỉnh từ các nghiên cứu trước đây với những sửa đổi nhỏ hoặc lớn.

Bảng 2.1. các hạng mục đo lường.

Xây dựng (Nguồn)	**Số biến**	**Hạng mục đo lường**	**Sửa đổi**
Nhận thức về ANM PMT: Nhận thức được lỗ hổng (Hina et al., 2019);	PV1	Tôi biết rằng tổ chức của tôi có thể dễ xuất hiện vi phạm bảo mật *(an ninh mạng),* nếu tôi không tuân thủ Chính sách Bảo mật Thông tin *(an ninh mạng)* của tổ chức tôi.	Sửa đổi lớn
	PV2	Tôi có thể trở thành nạn nhân của một cuộc tấn công có mục đích nếu tôi không tuân thủ Chính	Sửa đổi lớn

Li et at., 2019; Wong et at., 2022)		sách Bảo mật an toàn thông tin *(an ninh mạng)* của tổ chức tôi.	
	PV3	Về rủi ro bảo mật an toàn thông tin tại nơi làm việc của tôi, tài nguyên *(dữ liệu)* máy tính của tôi có thể dễ bị tấn công.	Sửa đổi lớn
	PV4	Tôi tin rằng mỗi cá nhân có ý thức và nỗ lực bảo vệ an toàn thông tin *(an ninh mạng)* của tổ chức, sẽ làm giảm nguy cơ truy cập bất hợp pháp và mất an toàn thông tin.	Sửa đổi lớn
	PV5	Các tổ chức nên đầu tư sử dụng các công nghệ bảo vệ an ninh mạng hiện đại.	Sửa đổi lớn
	PV6	Tổ chức cần thường xuyên thông báo cho nhân viên về các mối đe dọa an ninh mạng tiềm ẩn.	Sửa đổi lớn
	PV7	Nhiều nguy cơ tiềm ẩn về vi phạm bảo mật an toàn thông tin *(an ninh mạng)* sẽ xảy ra đối với hệ thống máy tính của tổ chức tôi.	Sửa đổi lớn
Nhận thức về ANM PMT: Hiệu quả của bản thân tự bảo mật (Hina et at., 2019; Li et at., 2022)	SE1	Tôi tin rằng tôi có các kỹ năng cần thiết để tự bảo vệ mình khỏi các hành vi vi phạm an toàn thông tin *(an ninh mạng)*.	Sửa đổi lớn
	SE2	Tôi tin rằng tôi đã phát triển khả năng ngăn chặn mọi người lấy cắp thông tin bí mật của tôi.	Sửa đổi lớn
	SE3	Tôi bật các biện pháp bảo mật *(tường lửa, chống vi-rút, v.v.)* trên tài nguyên máy tính công việc của mình.	Sửa đổi lớn
	SE4	Tôi tin rằng việc tự bảo vệ mình khỏi các hành vi vi phạm bảo mật an toàn thông tin *(an ninh mạng)*, nằm trong tầm kiểm soát của tôi.	Sửa đổi lớn

	SE5	Tôi tự tin khi mở duyệt trình web ở các mức độ bảo mật khác nhau.	Sửa đổi lớn
	SE6	Tôi cảm thấy tự tin khi xử lý các file bị nhiễm virus.	Sửa đổi lớn
	SE7	Tôi cảm thấy tự tin khi loại bỏ các phần mềm gián điệp và phần mềm độc hại khỏi máy tính.	Sửa đổi lớn
Nhận thức về ANM PMT: Hiệu quả đáp ứng (Hina et at., 2019; Li et at., 2019; Wong et at., 2022)	RE1	Trong tổ chức của tôi, những nỗ lực để đảm bảo an toàn thông tin *(an ninh mạng),* bí mật của tôi là có hiệu quả.	Sửa đổi lớn
	RE2	Tại tổ chức của tôi, các biện pháp bảo mật *(an ninh mạng)* hiện có để bảo vệ an toàn thông tin, công việc của tôi khỏi các vi phạm bảo mật *(an ninh mạng)* đều có hiệu lực.	Sửa đổi lớn
	RE3	Các biện pháp phòng ngừa an ninh mạng có sẵn cho tôi tại tổ chức của tôi, để đối phó với nội dung độc hại, đều có hiệu quả.	Sửa đổi lớn
	RE4	Các biện pháp bảo mật an toàn thông tin *(an ninh mạng)* tại tổ chức của tôi đã ngăn chặn tin tặc truy cập vào thông tin cá nhân hoặc giáo dục nhạy cảm.	Sửa đổi lớn
	RE5	Việc tuân thủ các chính sách bảo mật an toàn thông tin trong tổ chức sẽ ngăn chặn các vi phạm bảo mật an toàn thông tin, an ninh mạng.	Sửa đổi lớn
	RE6	Nếu tôi tuân thủ các chính sách bảo mật thông tin *(an ninh mạng)*, khả năng xảy ra vi phạm an toàn thông tin *(an ninh mạng)* sẽ giảm xuống.	Sửa đổi lớn
	RE7	Tuân thủ cẩn thận các chính sách bảo mật thông tin giúp tránh các vấn đề về an ninh mạng.	Sửa đổi lớn

	RE8	Tổ chức có thể cải thiện an toàn thông tin *(an ninh mạng)* khi người dùng chỉ ra được sơ suất về bảo mật *(an ninh mạng)* của họ đến tình hình an ninh mạng của tổ chức.	Sửa đổi lớn
	RE9	Tổ chức nên có Quy định chung về Bảo vệ Dữ liệu *(an ninh mạng).*	Sửa đổi lớn
	RE10	Tổ chức nên thường xuyên nâng cấp phần mềm chống vi-rút và tường lửa.	Sửa đổi lớn
Truyền thông của chính phủ (Tang et at., 2021)	GSM1	Tôi luôn đọc và nghe các khuyến cáo về an ninh mạng được Chính phủ đăng tải.	Sửa đổi nhỏ
	GSM2	Tôi luôn chia sẻ các khuyến cáo về an ninh mạng được Chính phủ đăng tải.	Sửa đổi nhỏ
	GSM3	Tôi luôn truyền đạt các khuyến cáo về an ninh mạng được Chính phủ đăng tải.	Sửa đổi nhỏ
Động lực bảo vệ thông tin (Ma, 2022; Posey et at., 2015)	IPM1	Tôi dự định bảo vệ tổ chức của mình khỏi các mối đe dọa về an toàn thông tin *(an ninh mạng)*.	Sửa đổi lớn
	IPM2	Mức độ thành công trong việc ngăn chặn các mối đe dọa về an ninh mạng, bảo mật thông tin của tổ chức là rất cao.	Sửa đổi lớn
	IPM3	Tôi luôn sẵn sàng tham gia vào các hoạt động bảo vệ hệ thống thông tin khỏi các mối đe dọa an ninh mạng.	Sửa đổi lớn
	IPM4	Tôi luôn nỗ lực bảo vệ tổ chức của mình khỏi các mối đe dọa về bảo mật thông tin *(an ninh mạng)*.	Sửa đổi lớn

	IPM5	Tôi sẽ cố gắng hết sức để ngăn chặn các mối đe dọa về bảo mật thông tin *(an ninh mạng)* xảy ra trong tổ chức của mình.	Sửa đổi lớn
Hành vi bảo vệ của nhân viên (Li et at., 2019)	EPB1	Tuân thủ Chính sách Bảo mật Thông tin *(an ninh mạng)* của tổ chức tôi là điều cần thiết.	Sửa đổi lớn
	EPB2	Tôi cảm thấy rằng việc phải tuân thủ Chính sách *(an ninh mạng)* Bảo mật Thông tin là hợp lý.	Sửa đổi lớn
	EPB3	Việc tuân thủ Chính sách *(an ninh mạng)* Bảo mật Thông tin của tổ chức tôi là một hành động quan trọng.	Sửa đổi lớn
Thái độ tuân thủ an ninh mạng (Hina, 2019)	ATT1	Tuân thủ Chính sách Bảo mật Thông tin *(an ninh mạng)* của tổ chức tôi là điều cần thiết.	Sửa đổi lớn
	ATT2	Tôi cảm thấy rằng việc phải tuân thủ Chính sách *(an ninh mạng)* Bảo mật Thông tin là hợp lý.	Sửa đổi lớn
	ATT3	Việc tuân thủ Chính sách *(an ninh mạng)* Bảo mật Thông tin của tổ chức tôi là một hành động quan trọng.	Sửa đổi lớn

4.2 Thu thập dữ liệu

Từ tháng 10 năm 2022 đến tháng 3 năm 2023, các phiếu khảo sát tự điền đã được gửi đến nhiều nhân viên đang làm việc tại các tỉnh, thành phố lớn ở Việt Nam như Thành phố Hồ Chí Minh, Hà Nội, tỉnh Đồng Nai và Bình Dương…, sử dụng ít nhất một nền tảng truyền thông xã hội như Facebook, Zalo, Viber, YouTube, TikTok và Instagram. Trong số 700 bảng câu hỏi được phân phát, có 564 bảng được trả lại và 323 bảng trong số đó được cho là phù hợp để điều tra. Số mẫu được xác định là đủ dựa trên Hair et at. (2014). Các bảng câu hỏi thỏa mãn một trong các điều kiện sau sẽ bị loại bỏ vì không hợp lệ:

- Nếu người trả lời có tất cả câu trả lời đưa ra kết quả giống nhau cho tất cả các câu hỏi (ví dụ: tất cả 1 hoặc tất cả 7); hoặc
- Nếu người trả lời hoàn thành cuộc khảo sát trong vòng chưa đầy 2 phút (Collier & Sherrell, 2009).

Chúng tôi sử dụng phép thử - để so sánh các đặc điểm nhân khẩu học của người trả lời đầu tiên và người trả lời cuối cùng, như được khuyến nghị trong các tài liệu trước đây, nhằm loại trừ bất kỳ thành kiến tiềm ẩn nào khi không phản hồi (Collier & Sherrell., 2009; Han et at., 2017). Bởi vì chúng tôi không tìm thấy sự khác biệt rõ rệt nào giữa hai nhóm người trả lời nên chúng tôi tin rằng thành kiến không phản hồi không phải là vấn đề.

4.3 Phương pháp nghiên cứu

Trong nghiên cứu này, mô hình nghiên cứu được xác định thông qua việc sử dụng phân tích mô hình phương trình cấu trúc bình phương nhỏ nhất từng phần (PLS-SEM) vì một số lý do. *Đầu tiên*, nó phù hợp hơn cho việc hồi quy bằng hòa giải so với các phương pháp khác. *Thứ hai*, nó tính đến sai số đo lường và đưa ra ước tính chính xác về các tác động trung gian (Chin, 1998b). Nó cũng thích hợp cho cả khung đơn giản và phức tạp và không yêu cầu giả định về tính quy chuẩn của dữ liệu (Hair et at., 2014). *Thứ ba*, PLS-SEM được coi là phù hợp hơn phương pháp hồi quy bình phương tối thiểu thông thường khi có các vấn đề như thiếu giá trị hoặc đa cộng tuyến và cỡ mẫu nhỏ. Cuối cùng, nó cũng được sử dụng rộng rãi trong bối cảnh hành vi bảo mật thông tin (Ma., 2022; Wong et at., 2022).

5. Kết quả và thảo luận

Phần mềm Smart PLS 4.0 được sử dụng để nghiên cứu mô hình nghiên cứu. Sau khi thực hiện phân tích mô tả, chúng tôi sử dụng kỹ thuật phân tích hai giai đoạn (Hair et at., 2014).

5.1 Phân tích mô tả

Bảng 2.2 dưới đây mô tả thông tin chi tiết về đặc điểm nhân khẩu học của người trả lời, dựa trên việc thu thập dữ liệu.

Bảng 2. 2. Đặc điểm nhân khẩu học của người trả lời

Mục nhân khẩu học		Số mẫu.	Tỷ lệ phần trăm (%)
Giới tính	Nam	239	74.0
	Nữ	84	26.0
Độ tuổi	18-35 tuổi	232	71.9
	36-45 tuổi	72	22.3
	Trên 45 tuổi	19	5.9
Trình độ học vấn	Trung học phổ thông	90	27.9
	Đại học	180	55.7
	Sau đại học	53	16.4
Kinh nghiệm làm việc	Dưới 3 năm	48	14.9
	3 đến 5 năm	56	17.3
	Hơn 5 năm	219	67.8
Quy mô tổ chức	Dưới 50 nhân viên	97	30.0
	51 đến 100 nhân viên	57	17.6
	Hơn 100 nhân viên	169	52.4

Bảng 2.3 hiển thị giá trị trung bình và độ lệch chuẩn cho từng biến. Tất cả những người tham gia khảo sát được yêu cầu mô tả nhận thức của họ bằng thang điểm 7, từ 1 (hoàn toàn không đồng ý) đến 7 (hoàn toàn đồng ý). Tuân thủ an ninh mạng ATT có số điểm cao nhất, với điểm trung bình là 6,283 trên

7,0 và độ lệch chuẩn là 1,114. SE có điểm thấp nhất, trung bình là 5,554 trên 7,0 và độ lệch chuẩn là 1,625.

5.2 Đánh giá mô hình đo lường

Giá trị hội tụ và giá trị phân biệt được áp dụng trong việc kiểm định các mô hình đo lường. Các biến chính trong nghiên cứu này được đánh giá bằng hệ số Cronbach's alpha (độ tin cậy xây dựng). Mỗi hệ số Cronbach's alpha trong nghiên cứu này từ 0,914 đến 0,949, vượt ngưỡng 0,7 (Kannan & Tan., 2005). Hơn nữa, tất cả các hệ số độ tin cậy tổng hợp (CR) đều có giá trị từ 0,946 đến 0,964, vượt quá giá trị đề xuất là 0,7 (Gefen et at., 2000). Do đó, như đã thấy trong Bảng 2.3 , độ tin cậy của cấu trúc được thỏa mãn vì CR và Cronbach's alpha về cơ bản không có lỗi đối với mỗi cấu trúc.

Sử dụng hệ số tải, chúng tôi đã đánh giá độ tin cậy của chỉ báo. Ngoài việc được nắm bắt trong các cấu trúc, các điều kiện còn được bao hàm bởi tải trọng lớn quan sát được trên các cấu trúc tương ứng ngay cả khi các chỉ số liên quan có cơ sở chung (Hair et at., 2014). Tất cả các mục trong Bảng 2.3 đều có hệ số tải trên giá trị khuyến nghị là 0,7, ngoại trừ RE10, bị loại khỏi thang đo vì giá trị tải thấp.

Nghiên cứu sử dụng giá trị trích xuất phương sai trung bình (AVE) làm phương tiện để đánh giá giá trị hội tụ. Mỗi AVE có giá trị từ 0,642 đến 0,899, trên ngưỡng đề xuất là 0,50 (Hair., 2011). Những phát hiện được trình bày trong Bảng 2.3 cho thấy rằng tất cả các cấu trúc đều đáp ứng thành công các tiêu chí về giá trị hội tụ.

5.3 Độ lệch phương pháp phổ biến

Bảng 2.3 Đánh giá mô tả và đo lường

Tên biến	*Ký hiệu*	*Hệ số tải (> 0 , 5)*	*Độ lệch chuẩn*	*Tiêu chuẩn*	*Alpha (> 0 , 7)*	*CR (> 0, 77)*	*AVE (> 0 , 5)*	*FCVIF (<3,3)*

Phương tiện truyền thông xã hội của chính phủ (GSM)	GSM1	0,933	5,922	1,382	0,935	0,958	0,885	2,382
	GSM2	0,964						
	GSM3	0,924						
Lỗ hổng nhận thức về mối đe dọa (PV)	PV1	0,825	6,147	1,275	0,937	0,948	0,725	2,144
	PV2	0,866						
	PV3	0,822						
	PV4	0,871						
	PV5	0,889						
	PV6	0,863						
	PV7	0,820						
Năng lực bản thân (SE)	SE1	0,854	5,554	1,625	0,942	0,953	0,743	2,311
	SE2	0,901						
	SE3	0,834						
	SE4	0,896						
	SE5	0,906						
	SE6	0,814						
	SE7	0,826						
Hiệu quả đáp ứng (RE)	RE1	0,857	6,013	1,313	0,938	0,947	0,642	1,414
	RE2	0,846						
	RE3	0,822						
	RE4	0,812						
	RE5	0,791						
	RE6	0,813						
	RE7	0,810						
	RE8	0,845						

	RE9	0,737						
	RE10	Đã xóa						
Thái độ tuân thủ an ninh mạng (ATT)	ATT1	0,942	6,283	1,114	0,944	0,964	0,899	1,911
	ATT2	0,955						
	ATT3	0,948						
Động lực bảo vệ thông tin (IPM)	IPM1	0,908	6,114	0,250	0,949	0,961	0,830	2,352
	IPM2	0,891						
	IPM3	0,903						
	IPM4	0,932						
	IPM5	0,921						
Hành vi bảo vệ nhân viên (EPB)	EPB1	0,917	5,957	1,401	0,914	0,946	0,854	1,124
	EPB2	0,937						
	EPB3	0,919						

Nguồn: Được tạo bởi các tác giả.

Nhiều nhà nghiên cứu khác nhau đã phát hiện ra rằng cộng tuyến hoàn toàn có thể được sử dụng để xác định độ lệch phương pháp chung (CMB). Dựa theo (Kock., 2015) , nếu giá trị cộng tuyến đầy đủ (FCVIF) nhỏ hơn 3,3 thì dữ liệu không có bất kỳ vấn đề CMB nào. Như được hiển thị trong Bảng 2.3, tất cả các cấu trúc tiềm ẩn trong dữ liệu đều có FCVIF dưới 3,3, cho thấy không có bất kỳ vấn đề CMB nào.

Để đánh giá giá trị phân biệt, chúng tôi sử dụng tỷ lệ Fornell - Larcker và dị tính - đơn tính (HTMT) (được hiển thị trong Bảng 2.4). Căn bậc hai của AVE trên các đường chéo cao hơn so với căn bậc hai của mối tương quan giữa các cấu trúc (hàng và cột tương ứng), thường là dấu hiệu cho thấy mối tương quan chặt chẽ giữa các cấu trúc và các chỉ số tương ứng của chúng (Chin., 1998a, 1998b; Fornell and Larcker., 1981). Ngoài ra, khi giá trị HTMT cao hơn ngưỡng 0,85, sẽ

phát sinh các vấn đề quan trọng về giá trị phân biệt. Tuy nhiên, mối tương quan giữa các cấu trúc ngoại sinh và mọi HTMT đều thấp hơn 0,85. Kết quả là, giá trị phân biệt của tất cả các cấu trúc được xác nhận thỏa đáng.

5.4 Nhận xét mô hình kết cấu

Để kiểm tra các mô hình cấu trúc, chúng tôi sử dụng kỹ thuật khởi động để tính toán các giá trị beta *(b), R 2* và các giá trị - tương ứng cho việc lấy mẫu lại là 5.000 (Hair et at., 2014). Việc tính toán R^2 được thực hiện để đánh giá khả năng dự báo của mô hình kết cấu. Hệ số xác định (R^2) định lượng tỷ lệ phương sai trong các biến nội sinh có thể quy cho biến ngoại sinh. Dựa theo Cohen. (1988), R^2 giá trị của

Bảng 2.4. Tỷ lệ HTMT và tiêu chí Fornell-Larcker

Tiêu chí Fornell-Larcker

	ATT (1)	EPB (2)	GSM (3)	IPM (4)	PV (5)	RE (6)	SE (7)
(1)	**0,948**						
(2)	0,674	**0,924**					
(3)	0,695	0,773	**0,941**				
(4)	0,824	0,805	0,735	**0,911**			
(5)	0,721	0,692	0,612	0,776	**0,851**		
(6)	0,732	0,686	0,708	0,779	0,757	**0,801**	
(7)	0,558	0,669	0,679	0,650	0,654	0,765	**0,862**

Tỷ lệ HTMT

(1)							
(2)	0,723						
(3)	0,737	0,837					
(4)	0,869	0,862	0,779				
(5)	0,761	0,742	0,650	0,818			
(6)	0,776	0,733	0,748	0,822	0,810		
(7)	0,581	0,720	0,720	0,685	0,688	0,800	

Lưu ý: Căn bậc hai của AVE được in đậm trên các đường chéo
Nguồn: Được tạo bởi các tác giả.

0,75, 0,50 hoặc 0,25 đối với các biến tiềm ẩn nội sinh trong mô hình cấu trúc có thể được mô tả tương ứng là đáng kể, trung bình hoặc thấp. Những phát hiện thu được từ Bảng 2.5 chứng minh rằng giá trị R^2 của các cấu trúc nội sinh nằm trong phạm vi dung sai được chỉ định. Do đó, những kết quả này chỉ ra rằng mô hình có mức độ chính xác dự đoán tương đối cao về tổng thể.

Ngoài ra, chúng tôi đánh giá tầm quan trọng của độ lớn của các hệ số cấu trúc. Cohen. (1988) cho rằng f^2 giá trị 0,02, 0,15 và 0,35 tương ứng là tác động yếu, trung bình và mạnh. Như được trình bày trong Bảng 2.5, mức độ ảnh hưởng của các mối liên kết được kiểm tra nằm trong phạm vi mạnh, ngoại trừ trường hợp yếu khi mức độ ảnh hưởng của các kết nối giữa ATT với EPB bằng 0,002.

5.5 Kiểm tra giả thuyết

Việc đánh giá SEM trong Hình 2.1 và Bảng 2.5 cho thấy kết quả của việc kiểm tra giả thuyết, xác nhận tất cả các giả thuyết. Sự tham gia vào GSM dự đoán một cách có ý nghĩa PV, SE, RE và ATT tuân thủ an ninh mạng; tất cả các giá trị p đều nhỏ hơn 0,001, do đó, *H1* - *H4* được xác nhận. Những phát hiện này tương tự với những phát hiện của PV và RE, cả hai đều có ảnh hưởng đáng kể đến ATT tuân thủ an ninh mạng. Do đó, cả *H5* và *H7* đều được xác nhận và SE dự đoán một cách có ý nghĩa sự tuân thủ an ninh mạng ATT, vì vậy *H6* được xác nhận. Tuy nhiên, đường dẫn là âm, với giá trị - thấp hơn 0,05, cho thấy SE có tác động tiêu cực đến ATT tuân thủ an ninh mạng. *H8* và *H10* được hỗ trợ, với giá trị p nhỏ hơn 0,001, điều này cho thấy rằng ATT tuân thủ an ninh mạng dự đoán đáng kể IPM và EPB. *H9* được hỗ trợ vì IPM có ảnh hưởng đáng kể đến EPB.

Chúng tôi ước tính các tác động gián tiếp để xác định: tác động trung gian của PV, SE và RE đối với mối quan hệ giữa GSM và ATT và tác động trung gian của IPM đối với mối quan hệ giữa ATT và EPB (xem Bảng 2.6). Kết quả chỉ ra rằng tất cả các yếu tố đều đóng vai trò trung gian một phần trong hai mối quan hệ.

Bảng 2.5 kết quả kiểm tra giả thuyết.

Giả thuyết	Mối quan hệ	Tiêu chuẩn β	Giá trị t	Giá trị p	R^2	f^2	Kết quả
H1	GSM → ATT	0,350	13,220	0,000	0,653	0,160	Chấp nhận
H2	GSM → PV	0,612	9,291	0,000	0,373	0,600	Chấp nhận
H3	GSM → SE	0,679	14,746	0,000	0,459	0,855	Chấp nhận
H4	GSM → RE	0,708	13,972	0,000	0,500	1,006	Chấp nhận
H5	PV → ATT	0,360	3,656	0,000	0,653	0,154	Chấp nhận
H6	SE → ATT	-0,184	2,435	0,015		0,037	Chấp nhận
H7	RE → ATT	0,352	3,508	0,000		0,099	Chấp nhận
H8	ATT → IPM	0,824	17,001	0,000	0,677	2,109	Chấp nhận
H9	IPM → EPB	0,776	10,517	0,000	0,646	0,551	Chấp nhận
H10	ATT → EPB	0.035	11,412	0,000		0,002	Chấp nhận

Nguồn: Được tạo bởi các tác giả.

5.6 Thảo luận

Điều tra này góp ý đáng kể cho lĩnh vực bảo mật thông tin bằng cách cung cấp một nhận xét toàn diện về tác động của GSM đối với ATT và EPB của nhân viên đối với bảo mật thông tin. Nó xem xét một số khía cạnh, bao gồm thái độ, động cơ và hành vi, từ góc độ rộng hơn, đáp ứng lợi ích của cả các học giả và những người thực hành bảo mật thông tin. Những khám phá này cung cấp bằng chứng mạnh mẽ để hỗ trợ 10 giả thuyết.

Ban đầu, sự tham gia của GSM có kết quả tích cực trong việc thúc đẩy thái độ tích cực đối với việc tuân thủ an ninh mạng. Cụ thể hơn, nó đóng vai trò thúc đẩy thái độ tích cực của nhân viên đối với việc tham gia vào các hành vi bảo vệ. Kết quả này phù hợp với điều tra trước đây (Hermann et at., 2020; Yin et at., 2022), lập luận rằng việc sử dụng thường xuyên mạng xã hội sẽ nâng cao thái độ tích cực đối với các hành vi bảo vệ.

Bảng 2.6 hiệu ứng trung gian

Mối quan hệ	Loại	Ước tính	Giá trị - T	Giá trị - P	Nhận xét
H6. GSM → ATT	Trực tiếp	0.350	13.220	0.000	Chấp nhận
GSM → PV → ATT	Gián tiếp	0.220	3.082	0.002	Bổ sung
GSM → SE → ATT	Gián tiếp	-0.125	2.369	0.018	Bổ sung
GSM → RE → ATT	Gián tiếp	0.249	3.188	0.001	Bổ sung
H10. ATT → EPB	Trực tiếp	0.035	11.412	0.000	Chấp nhận.
ATT → IPM → EPB	Gián tiếp	0.639	9.123	0.000	Bổ sung

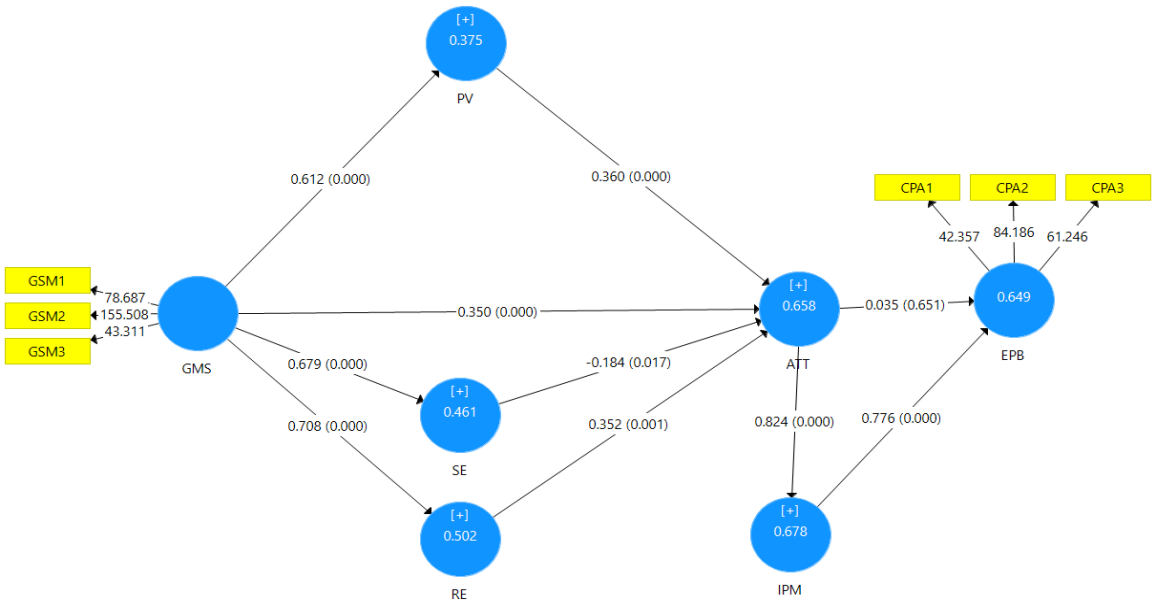
Nguồn: Được tạo bởi các tác giả.

Ngoài ra, việc tham gia vào GSM có tác động tích cực đến PV, RE và SE, điều này ngụ ý rằng mọi người tham gia vào GSM nội dung liên quan đến bảo mật càng lâu thì họ càng cảm thấy dễ bị tổn thương trước các mối đe dọa về rủi ro bảo mật thông tin và SE của chính họ cũng như RE khi đối mặt với những rủi ro như vậy. Những khám phá của chúng tôi tương ứng với những điều tra trước đó (Intravia et at., 2017; Kim & Hawkins., 2020; Shah et at., 2020; Tang et at., 2021; Tu et at., 2015).

Thứ hai, chúng tôi nhận thấy rằng ATT bị ảnh hưởng tích cực bởi PV và RE. Những phát hiện này phù hợp với những phát hiện trong các nghiên cứu trước đây (Anderson & Agarwal., 2010; Hina et at., 2019; Ifinedo., 2012; Wong et at., 2022). Tuy nhiên, những khám phá thực nghiệm chứng minh rằng PV và RE có tác động tích cực đến ATT. Ngược lại, SE có tác động tiêu cực đến ATT. Phát hiện này ngụ ý rằng mọi người ít có xu hướng tuân thủ tốt các giao thức ANM khi họ tin rằng họ có thể thực hiện các biện pháp quy định và quản lý hiệu quả các mối hiểm họa tiềm ẩn. Điều này đặc biệt liên quan đến năng lực và khả năng phán đoán của họ trong việc giải quyết các mối nguy hiểm liên quan đến vi phạm an ninh. Phát hiện này góp phần tạo ra các kết quả chủ yếu là hỗn hợp vì nó phù hợp với một số điều tra (Hooper & Blunt., 2020; Moody et at., 2018), nhưng không phải những người khác (Anderson and Agarwal, 2010; Johnston & Warkentin., 2010).

Cuối cùng, chúng tôi thấy rằng IPM về cơ bản được lý giải tích cực bởi ATT của nhân viên đối với việc tuân thủ. Mối quan hệ giữa hai khía cạnh này cho thấy rằng nhân viên có động lực hơn để dành thêm thời gian và nỗ lực để bảo vệ tài sản thông tin khi họ thường có thái độ tích cực hơn đối với các hành vi bảo vệ. Phát hiện này phù hợp với những phát hiện trong các điều tra trước đây (Hina et at., 2019; Ma., 2022; Martens et at., 2019; Safa et at., 2015; Wu, 2020). Ngoài ra, chúng tôi thấy rằng IPM sau đó có tác động đáng kể đến EPB, điều này phù hợp với những phát hiện trước đó (Lebek et at., 2014; Siponen

et at., 2014; Warkentin et at., 2016). Cụ thể, những nhân viên có động lực bảo vệ an ninh thông tin cao hơn sẽ có xu hướng tham gia vào các hành vi giảm thiểu rủi ro bảo mật.



Hình 2.2 Kết quả kiểm tra giả thuyết.

Nguồn: Được tạo bởi các tác giả.

6. Ý nghĩa và kết luận

6.1 Đóng góp về mặt lý thuyết

Nghiên cứu này bổ sung thêm kiến thức bằng cách cung cấp nhiều giải thích mang tính lý thuyết về kết quả của việc sử dụng PMT và CT trong các tình huống an ninh mạng. Đầu tiên, mặc dù các EPB bảo mật thông tin đã được điều tra rộng rãi liên quan đến tiến bộ công nghệ, nhưng điều tra về các hành vi này liên hệ đến tác động của GSM vẫn còn ở giai đoạn sơ khai. Một số điều tra đã xem xét cách tốt nhất để bảo vệ con người khỏi các mối đe dọa an ninh với sự hỗ trợ của GSM, mặc dù nhiều nghiên cứu đã được thực hiện trong bối

cảnh tổ chức (Johnston & Warkentin, 2010; Warkentin et al., 2016) và bối cảnh cá nhân (Liang & Xue, 2010; Martens et at., 2019; Tu et at., 2015). Điều này rất quan trọng vì mạng xã hội là nền tảng mạnh mẽ để các chính phủ và tổ chức quốc tế sử dụng nhằm nâng cao kiến thức cho công chúng và đưa ra đề xuất về cách ngăn chặn việc trở thành nạn nhân của tội phạm mạng (Beaunoyer et at., 2020; Chen et at., 2020; Farooq et at., 2020). Nghiên cứu này bổ sung thêm kiến thức về ảnh hưởng của GSM đến bảo mật thông tin hành vi bằng cách kiểm tra ảnh hưởng của GSM đối với các biến PMT và EPB.

Thứ hai, thay vì kiểm tra sự thay đổi hành vi thực tế, các nghiên cứu về bảo mật thông tin hiện tại chủ yếu tập trung vào ý định liên quan đến bảo mật. Họ khẳng định rằng, mặc dù PMT chủ yếu xoay quanh các ý định nhưng nó đã được mở rộng một cách hiệu quả để bao gồm các hoạt động hữu hình. Nghiên cứu này chứng minh tầm quan trọng của việc nhân viên thực hiện các hành vi bảo vệ an ninh thông tin thực tế nhằm nâng cao các hành vi này, cũng như trong việc thúc đẩy thái độ tuân thủ và động lực bảo vệ. Việc đo lường toàn diện về thái độ, động cơ và hành vi tạo điều kiện cho sự hiểu biết sâu sắc hơn về các cơ chế thông qua đó các hành vi bảo vệ được phát triển (Flood et at., 2006).

Thứ ba, chủ đề của chúng tôi là điều tra tiên phong về ảnh hưởng của mạng xã hội đối với hiệu quả tuyên truyền. Ngược lại, các điều tra trước đây chủ yếu tập trung vào ảnh hưởng của các phương tiện thông tin đại chúng thông thường như truyền hình và báo chí, tác động lên quan nhận thức và thái độ của cá nhân (Hermann et at., 2020; Tang et at., 2021). Ngoài việc xem xét tác động lan tỏa của mạng xã hội, điều tra của chúng tôi còn đặc biệt xem xét hậu quả của tài khoản GSM. Chúng tôi thấy rằng thông qua các yếu tố PMT, GSM có cả ảnh hưởng trực tiếp và gián tiếp đến thái độ của những người theo dõi trên khắp PV, SE và RE. Hơn nữa, IPM đóng vai trò trung gian giải thích một phần trong mối tương quan giữa ATT và EPB.

Cuối cùng, việc kết hợp CT vào điều tra của chúng tôi sẽ mở rộng kiến thức hiện có về PMT, vốn đã được xem xét trong các bài báo trước. Ngược lại với một nghiên cứu khác (Tu et at., 2015), nhấn mạnh tầm quan trọng của việc đánh giá các mối đe dọa và cơ chế đối phó để thực hiện các biện pháp an ninh trong hệ thống tổ chức, điều tra này trình bày một mô hình phức tạp hơn, xem xét cụ thể các nhân tố ảnh hưởng đến đánh giá của cá nhân về các mối đe dọa và chiến lược đối phó trong bối cảnh cá nhân. Kết quả phân tích dữ liệu cung cấp bằng chứng ủng hộ cho tất cả các giả thuyết của chúng tôi, cho thấy rằng PMT và lý thuyết CT giải thích một cách hiệu quả cho hành vi có trách nhiệm. Chúng tôi mở rộng việc áp dụng các lý thuyết này vì chúng được chứng minh là có khả năng giải thích trong khuôn khổ điều tra đang diễn ra. Ngoài ra, chúng còn đóng vai trò là nền tảng để ước tính các mối đe dọa chính và chiến lược đối phó.

6.2 Hàm ý quản trị

Thứ nhất, nghiên cứu có nhiều ý nghĩa thực tiễn đối với các chuyên gia trong lĩnh vực này. Phát hiện của chúng tôi nhấn mạnh tầm quan trọng của an ninh mạng trong bối cảnh chuyển đổi kỹ thuật số. Các nhà điều hành ngày càng tập trung vào các mối lo ngại về an ninh mạng liên quan đến các nhóm làm việc từ xa, bên cạnh việc nhận thức được tầm quan trọng của năng suất của nhóm làm việc từ xa. Nghiên cứu của chúng tôi cung cấp cho các chuyên gia những hiểu biết sâu sắc về vai trò tiềm năng của phương tiện truyền thông xã hội trong việc tạo điều kiện phổ biến thông tin nhằm giảm thiểu rủi ro an ninh mạng. Nghiên cứu của chúng tôi nhấn mạnh thêm tầm quan trọng của việc tự vệ đối với người dùng cá nhân. Do đó, các học viên bắt buộc phải tích cực ủng hộ việc áp dụng các biện pháp bảo vệ an ninh mạng để tăng cường -các biện pháp tự bảo vệ chủ động. Một số biện pháp này bao gồm việc sử dụng các quy trình đăng nhập phức tạp hơn (thông tin xác thực và mật khẩu; xác minh hai bước; mật khẩu), cũng như sử dụng các trình duyệt web có thể

lưu trữ mật khẩu, tuân theo quy trình đăng nhập hoặc mật khẩu chính của riêng chúng.

Thứ hai, bằng chứng thực nghiệm chứng minh quan điểm cho rằng thái độ và động cơ thực hiện các biện pháp bảo mật của người dùng bị ảnh hưởng đáng kể bởi những đánh giá của họ về các mối đe dọa và chiến lược đối phó. Các cơ quan chính phủ và các tổ chức khác được khuyến nghị cung cấp các chương trình đào tạo về bảo mật thông tin nhắm mục tiêu cụ thể đến các mối đe dọa bảo mật. Các chương trình này cần nhằm mục đích tăng cường khả năng của các cá nhân, bao gồm cả nhân viên, để đánh giá hiệu quả các rủi ro bảo mật tiềm ẩn và sử dụng các biện pháp khắc phục thích hợp. Một số hoạt động quan trọng, chẳng hạn như phát động các chiến dịch thường xuyên nhằm giáo dục nhân viên về việc giảm thiểu sự hiện diện trên Internet, thúc đẩy sự an toàn của nhân viên và phát hiện các mối nguy hiểm nội bộ, là vô cùng quan trọng và cần được chứng thực. Khi các cá nhân nhận thấy mức RE cao hơn, họ có xu hướng sử dụng các kỹ thuật đối phó thành công hơn. Do đó, các cơ quan chính phủ bắt buộc phải phân phối các thông tin nhằm thúc đẩy việc sử dụng công nghệ có trách nhiệm và nâng cao hiệu quả trong việc giải quyết các vấn đề. Trong quá trình áp dụng, các tổ chức bắt buộc phải giải thích một cách hiệu quả các quy trình thực hiện của mình cho tất cả nhân viên. Để tăng cường thúc đẩy động lực bảo vệ, các công ty cần đảm bảo rằng các biện pháp được sử dụng được thực hiện một cách chính xác, có tổ chức và đơn giản. Sau đó, nhân viên sẽ có khả năng ưu tiên những phương pháp nào mang lại biện pháp bảo vệ tốt nhất trong nỗ lực không ngừng của họ nhằm quản lý và giảm thiểu nguy hiểm.

Thứ ba, những phát hiện của chúng tôi chứng minh thêm tác động gián tiếp của các biến PMT lên biến phụ thuộc của chúng tôi thông qua sự tham gia vào GSM. Điều này cho thấy GSM có thể có ảnh hưởng đáng kể đến hành vi của các cá nhân khi nói đến bảo mật thông tin như một phương tiện khai thác

kỹ thuật số. Các tổ chức chính phủ nên liên tục mở rộng sự tham gia của mình vào việc truyền bá thông tin chính xác và thích hợp về GSM của họ. Để đảm bảo tác động tối đa, những tin nhắn GSM này phải được soạn thảo và lựa chọn cẩn thận. Các vấn đề an toàn thông tin có thể có tác động xã hội bất lợi vì các đánh giá về mối đe dọa và cách đối phó trong tổ chức có hiệu quả. Do đó, chúng tôi đặc biệt khuyên bạn nên gửi những thông báo chia sẻ các ví dụ liên quan về những lo ngại nghiêm trọng về bảo mật thông tin. Các tổ chức chính phủ phải liên tục quảng bá giá trị của việc bảo vệ an ninh thông tin và nhấn mạnh đến lỗ hổng của các hành động không bảo vệ khi xây dựng thông điệp.

Cuối cùng, việc tạo ra thái độ và động lực tích cực có thể cải thiện các hành vi bảo vệ là điều cần thiết vì các vi phạm an ninh là rất quan trọng và quan trọng đối với doanh nghiệp, như nghiên cứu của chúng tôi đã chỉ ra. Các nhóm và nhân viên quản lý rủi ro là những người đóng vai trò thiết yếu và là người bảo vệ khả năng phục hồi không gian mạng vì hầu hết các công ty vẫn đang trong giai đoạn đầu của quá trình số hóa. Nhân viên cần lưu ý rằng bảo vệ an ninh mạng là nhiệm vụ chung giữa các nhân viên và phòng ban của tổ chức. Mọi người có kết nối Internet đều bị ảnh hưởng. Để cải thiện tình trạng ANM của mình, các tổ chức nên nhấn mạnh tầm quan trọng và lợi ích của các hành vi phòng ngừa ANM.

6.3. Kết luận

Việc chuyển đổi kỹ thuật số đã đồng thời cung cấp cho các quan chức chính phủ các kênh hiệu quả để giao tiếp với công chúng và gây ra những lo ngại đáng kể về an ninh cho bất kỳ tổ chức nào. Bài viết này trình bày nghiên cứu mới cho thấy các hành vi bảo vệ an ninh thông tin được hình thành như thế nào dựa trên ảnh hưởng của GSM, thái độ bảo mật thông tin và động cơ bảo vệ. Để điều tra vai trò của GSM trong việc tác động đến hành vi bảo mật thông tin của người dùng đối với các mối lo ngại về bảo mật thông tin, chúng

tôi đặc biệt sử dụng cả CT và PMT làm khung lý thuyết. Chúng tôi đánh giá thực nghiệm mô hình điều tra và giả thuyết đề xuất của mình bằng cách kiểm tra dữ liệu từ một cuộc khảo sát nhân viên Việt Nam tham gia GSM. Nghiên cứu của chúng tôi cho thấy rằng sự tham gia của người dùng vào GSM có tác động tích cực đến việc tuân thủ an ninh mạng ATT đối với việc sử dụng các biện pháp bảo mật thông qua PV và RE, nhưng lại có tác động tiêu cực thông qua SE. Ngoài ra, ATT tuân thủ an ninh mạng có tác động mạnh mẽ hơn đến EPB thông qua IPM so với tác động trực tiếp của nó. Phát hiện của chúng tôi khuyến khích điều tra sâu hơn về thực tiễn quản lý GSM và bảo mật thông tin, đồng thời cung cấp những hiểu biết thực tế cho những người thực hành.

6.4 Hạn chế và đề xuất nghiên cứu tiếp theo

Mặc dù nghiên cứu này đưa ra những quan điểm mới và hữu ích về cả lý thuyết và thực tiễn nhưng vẫn có một số hạn chế nhưng chúng đưa ra những hướng nghiên cứu tiếp theo. Đầu tiên, chúng tôi chỉ thu thập thông tin từ các nền tảng truyền thông xã hội nổi tiếng ở một quốc gia. Thiết kế của những nền tảng này và văn hóa dân tộc có thể làm sai lệch những phát hiện của chúng tôi. Để tăng tính khái quát cho nghiên cứu của chúng tôi, nghiên cứu trong tương lai có thể sử dụng cách tiếp cận đa văn hóa hoặc đa nền tảng. Thứ hai, mặc dù một phần đáng kể của phương sai trong biến phụ thuộc được giải thích bằng mô hình của chúng tôi, một số biến quan trọng khác, chẳng hạn như nhận thức về an ninh và chuẩn mực xã hội, không được tính đến. Để nâng cao hơn nữa sự hiểu biết về quản lý GSM và bảo mật thông tin người dùng, các cuộc điều tra trong tương lai có thể kết hợp các yếu tố này. Thứ ba, chúng tôi không kiểm tra xem liệu các yếu tố như tính cách, giới tính và tình trạng kinh tế xã hội có thể đóng vai trò là yếu tố điều tiết hay không. Những người điều hành tiềm năng này có thể làm sáng tỏ hơn về hành vi bảo mật thông tin của mọi

người. Vì lý do đó, điều tra trong tương lai nên xem xét những tác động điều tiết này.

Chương III. Từ nhận thức đến hành vi: Tìm hiểu việc tuân thủ an ninh mạng ở Việt Nam

Chương này được trình bày từ kết quả bài báo thứ hai đã được công bố:

Tran, D.V., Nguyen, P.V., Le, L.P. and Nguyen, S.T.N. (2024), "From awareness to behaviour: understanding cybersecurity compliance in Vietnam", *International Journal of Organizational Analysis*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/IJOA-12-2023-4147. Scopus Q2.

Từ những đóng góp thiết thực của bài báo thứ nhất đã khuyến nghị tới các cơ quan chính phủ và các tổ chức khác nên cung cấp các chương trình đào tạo, hay ban hành chính sách của tổ chức về bảo mật thông tin nhắm mục tiêu cụ thể đến các mối đe dọa bảo mật. Các chương trình này cần nhằm mục tiêu củng cố khả năng của các cá nhân để đánh giá hiệu quả các rủi ro bảo mật tiềm ẩn và sử dụng các biện pháp khắc phục thích hợp. Cho nên, ở điều tra thứ hai này chúng tôi xem xét những ảnh hưởng của CSA và ATT đối với các EPB của nhân viên.

Điều tra khám phá mối quan hệ giữa nhận thức về các biện pháp an ninh mạng và thái độ tuân thủ, đồng thời xem xét tác động của những yếu tố này đến hành vi bảo vệ tài sản và thông tin của tổ chức. Phương pháp định lượng được sử dụng, với dữ liệu sơ cấp thu thập từ bảng câu hỏi khảo sát nhân viên tại các tổ chức ở Việt Nam. Dữ liệu sau đó được phân tích bằng phương pháp mô hình cấu trúc bình phương nhỏ nhất từng phần (PLS-SEM). Kết quả cho thấy, chính sách và chương trình giáo dục nâng cao nhận thức về an ninh có mối liên hệ tích cực với CSA, đóng vai trò quan trọng trong việc hình thành thái độ và ý định tuân thủ chính sách bảo mật thông tin (ISPC). Thái độ tích cực liên quan đến ý định hướng tới ISPC và EPB của nhân viên. Điều tra này đóng góp vào hiểu biết về ANM ở các nước đang phát triển như Việt Nam,

cung cấp khuôn khổ toàn diện để hiểu ý định và hành vi bảo vệ thông qua CSA và ATT, mở rộng điều tra trước đây về tác động của các nhân tố này đối với EPB của nhân viên.

1. Giới thiệu

Công nghệ thông tin và truyền thông đang trải qua một sự thay đổi mạnh mẽ và sự trỗi dậy của Internet of Things đã dẫn đến một cuộc cách mạng về hệ thống vật lý không gian mạng và mang đến cho người dùng vô số lợi ích mới, đặc biệt là ở Việt Nam. Internet đã mở ra những cơ hội kinh tế mới cho các cá nhân và doanh nghiệp bằng cách hợp lý hóa quy trình thực hiện giao dịch qua thiết bị di động và tạo điều kiện kết nối với những người mới thông qua mạng xã hội (Lee et at., 2017; Saadatdoost et at., 2015). Các mục tiêu phát triển bền vững thường được coi là phương pháp giúp các nước đang phát triển nhanh chóng bắt kịp các nước phát triển (Michael et at., 2019). Do vai trò quan trọng của nó đối với nền kinh tế và xã hội nói chung, một số chính phủ đã coi Internet là một phần của cơ sở hạ tầng quan trọng của đất nước họ (Chang et at., 2020). Mặc dù sự mở rộng nhanh chóng của nó mở ra những con đường tiến bộ mới đầy hứa hẹn nhưng nó cũng gây ra một số rủi ro đáng lo ngại (Ani et at., 2017). Hơn nữa, trong lĩnh vực bảo mật, các mối đe dọa thường nhắm vào tài sản của tổ chức hơn là tài sản cá nhân (Menard et at., 2017). Chi phí quản lý rủi ro mạng trong trường hợp xảy ra một cuộc tấn công có thể rất lớn nếu không có biện pháp giảm thiểu rủi ro thỏa đáng, chiến lược xử lý sự cố và các chiến dịch nâng cao nhận thức về an ninh mạng hiệu quả (Wong et at., 2022). Kết quả là, các nghiên cứu về những thực tiễn tốt nhất để thiết lập và duy trì năng lực mạng an toàn tại các tổ chức là rất cần thiết ở các nước kém phát triển.

Để đảm bảo doanh nghiệp có thể tiếp tục hoạt động an toàn và hiệu quả trong thời đại kỹ thuật số, điều quan trọng là phải đảm bảo rằng nhân viên có

động lực hành động theo cách tương thích với các chính sách bảo mật thông tin. Do sự đa dạng về nhân sự, quản lý, đối tác và cơ sở hạ tầng ở mọi tổ chức nên các lỗ hổng nội bộ rất khó kiểm soát (Sarkar, 2010). Các vi phạm an ninh nội bộ, dù cố ý hay vô tình, đều khó phát hiện và điều tra hơn bất kỳ mối đe dọa nào khác (Barlow et at., 2013). Đó là lý do tại sao điều quan trọng là phải xem xét điều gì khiến mọi người tuân thủ hệ thống bảo mật thông tin và bảo vệ chúng. Do đó, nếu nhân viên không được đào tạo đầy đủ về chủ đề an ninh mạng, công ty sẽ dễ bị tổn thương trước những mối đe dọa nghiêm trọng từ môi trường kinh doanh bên ngoài của họ. Sự thiếu nhận thức của họ có thể cho thấy hành vi tiêu cực hoặc phản kháng, có khả năng gây tổn hại đến sự an toàn của doanh nghiệp và dữ liệu của doanh nghiệp (BulgurCu et at., 2010; Donalds & Osei-Bryson., 2020; Hu et at., 2007). Ngoài ra, quan điểm tích cực về việc tuân theo các chính sách quản lý tính bảo mật của hệ thống thông tin là một dấu hiệu mạnh mẽ cho thấy nhân viên sẽ tuân theo chúng (Ifinedo., 2012; Venkatesh et at., 2003).

Do khả năng kết nối Internet ngày càng tăng, mức độ tinh vi và tần suất của các cuộc tấn công mạng đã tăng lên đáng kể. Việc tiếp tục hành vi bất lợi này đã gây ra những hậu quả tiêu cực đáng kể và sâu rộng, không chỉ ảnh hưởng đến các doanh nghiệp, toàn bộ các ngành mà còn cả chính phủ các quốc gia (Tran et at., 2024). Do đó, các chính phủ đã ban hành các biện pháp có mục tiêu để bảo vệ các mạng liên quan đến an ninh quốc gia. Mục tiêu là tăng cường cấu trúc pháp lý về an ninh thông tin mạng để đảm bảo bảo vệ vững chắc các thông tin quan trọng về quốc phòng. Để đạt được điều này, các chính phủ phải ưu tiên đánh giá về khả năng và chuyên môn thực tế của những người phụ trách mạng lưới. Hơn nữa, việc thiết lập một khuôn khổ pháp lý toàn diện là cần thiết để kiểm soát hiệu quả an toàn thông tin mạng, đặc biệt là giảm nguy cơ và chống lại các mối đe dọa trên phạm vi kỹ thuật số. Quốc hội Việt Nam đã thông qua Luật ANM vào ngày 12 tháng 6 năm 2018 và có hiệu lực

từ ngày 1 tháng 1 năm 2019. Mục tiêu của luật này là giám sát các hoạt động nhằm duy trì trật tự, an ninh xã hội trong lĩnh vực kỹ thuật số, quy định cụ thể trách nhiệm của các cơ quan hữu quan, tổ chức và cá nhân. Tuy nhiên, điều cần thiết là phải tiến hành điều tra sâu hơn và tăng cường quản trị thể chế về các kế hoạch về an ninh, giáo dục và nâng cao nhận thức cũng như việc cung cấp các chính sách. Điều này là bắt buộc để đảm bảo an toàn cho nhân viên tại nơi làm việc trong quá trình sử dụng Internet và giao dịch trực tuyến.

Hành vi có chủ ý gắn chặt với cả nhận thức và thái độ về ANM (Burton-Howard et at., 2018; Wiafe et at., 2020), nhưng chỉ một số nghiên cứu toàn diện về nhận thức, thái độ, ý định và hành vi đã kết hợp các lý thuyết TPB và lý thuyết PMT với quản trị thể chế (IG). IG được chứng minh là được thúc đẩy mạnh mẽ bởi hành vi bảo vệ nhân viên trong việc tuân thủ chính sách (Hina et at., 2019). Tuy nhiên, người ta hiểu rất ít về cách các yếu tố này ảnh hưởng đến nhận thức của nhân viên, để lại một khoảng trống trong tài liệu mà nghiên cứu của chúng tôi lấp đầy bằng cách khám phá các yếu tố có thể truyền cảm hứng cho nhân viên tuân thủ các chính sách bảo mật và bằng cách khuyến khích khám phá và nâng cao nhận thức về thái độ của người đi trước. Do đó, trong nghiên cứu này, chúng tôi tích hợp TPB và PMT vào khung nghiên cứu để điều tra mối tương tác giữa CSA của nhân viên và thái độ đối với việc tuân thủ như một thước đo rõ ràng về hành vi bảo vệ nhân viên dưới sự quản lý của tổ chức. Cụ thể, chúng tôi giải quyết các câu hỏi điều tra sau:

1. Quản trị thể chế ảnh hưởng như thế nào đến CSA?

2. Tác động của CSA đối với mối quan hệ giữa EPB của nhân viên và ATT với vai trò trung gian do chủ ý đóng vai trò gì hướng tới việc tuân thủ chính sách bảo mật thông tin?

2. Cơ sở lý thuyết và phát triển giả thuyết

2.1. Lý thuyết Động cơ bảo vệ (PMT)

PMT được Rogers. (1975) giới thiệu lần đầu tiên để mô tả động cơ khuyến khích con người thực hiện hành vi bảo vệ khi họ gặp phải tín hiệu nguy hiểm. Nó cũng ngụ ý rằng mọi người có động cơ tham gia vào hoạt động tránh rủi ro vì họ muốn giữ an toàn cho bản thân (Guchev & Jordanovska-Gucheva, 2022). Cụ thể, lý thuyết này thừa nhận rằng khi các cá nhân phải đối mặt với khả năng xảy ra một kết quả tiêu cực, họ thường áp dụng một tập hợp các quy trình nhận thức nhất định để quyết định cách phản ứng. Hơn nữa, nó được cấu trúc theo hai quy trình: đánh giá mối hiểm họa và đánh giá khả năng ứng phó.

Đầu tiên, đánh giá mối hiểm họa là một quá trình hiểu biết mà mọi người sử dụng để đánh giá hiểm họa. Nó tính đến ba yếu tố quan trọng được coi là tiền đề của các hành động thích ứng của cá nhân: PV, PS và tính nhạy cảm với mối đe dọa (Rippetoe & Rogers., 1987). Thứ hai, đánh giá khả năng đối phó được mô tả là khả năng cá nhân để thực hiện các hành vi bảo vệ khi phải đối mặt với mỗi tình huống khó khăn. mối hiểm họa (Guchev & Jordanovska - Gucheva., 2022). Điều quan trọng là các nhân tố của đánh giá đối phó là hiệu quả ứng phó, tính tự hiệu quả và chi phí ứng phó (Li et at., 2019).

PMT đã được xác nhận trong tâm lý học (Floyd et at., 2000), nghiên cứu được thực hiện về bảo mật thông tin (Vance et at., 2012; Wall & Warkentin, 2019), sử dụng máy tính tại nhà (Tsai et at., 2016), người tiêu dùng (Kim et at., 2022) và việc áp dụng phần mềm chống đạo văn (Lee, 2011). Do đó, PMT cung cấp một khuôn khổ vững chắc để xây dựng mô hình điều tra nhằm lồng ghép nhận thức về ANM vào điều tra này.

2.2. Lý thuyết về Hành vi có kế hoạch (TPB)

TPB là một mô hình hành vi thường được sử dụng để giải thích và chỉ ra vai trò của động lực nội tại trong việc hình thành hành vi của con người. Hơn nữa, lý thuyết này cho rằng con người có lý trí, có niềm tin và kiến thức, những điều này có được một cách có hệ thống thông qua kinh nghiệm cá nhân, giáo dục chính quy, phương tiện truyền thông và tương tác với gia đình và bạn bè. Kết quả là họ có xu hướng diễn giải và ghi nhớ để xác định hành vi có chủ ý của mình. Thái độ cá nhân và chuẩn mực chủ quan về việc thực hiện một hành vi hình thành nên ý định hành vi, là yếu tố thiết yếu của hành vi thực tế (Ajzen, 1991). Cụ thể, TPB đã được áp dụng trong dịch vụ điện tử (Liao et at., 2007), công nghệ truyền thông (Moletsane & Tsibolane., 2020; Teo & Beng Lee., 2010; Yousufet at., 2023), truyền thông sức khỏe (Wu & Kuang., 2021) và bảo mật thông tin (Alanazi et at., 2022). Nghiên cứu này mở rộng khi TPB kiểm tra ảnh hưởng của thái độ và ý định đối với EPB của nhân viên.

2.3. Nhận thức về an ninh mạng

Tầm quan trọng của nhận thức về an ninh trong việc nhận thức các mối nguy hiểm đe dọa tài nguyên nơi làm việc cần được nhấn mạnh (Bulgurcu et at., 2010). Ngoài ra, nhận thức về bảo mật thông tin đề cập đến mức độ mà người dùng hiểu được tầm quan trọng của bảo mật thông tin và nghĩa vụ và hành động trong việc thực hiện đầy đủ các khía cạnh kiểm soát an ninh thông tin nhằm bảo mật dữ liệu và mạng của công ty (Shaw et at., 2009). Tương tự, CSA đề cập đến kiến thức và thực tiễn bảo mật cơ sở hạ tầng kỹ thuật số của một công ty (Alghamdi., 2021).

Năng lực bản thân, hiệu quả ứng phó và các rào cản được nhận thức đều được coi là những yếu tố quan trọng quyết định mức độ nhận thức về an ninh mạng (Alghamdi., 2021). PMT đóng vai trò là nền tảng cho sự phát triển của cấu trúc này, được thể hiện là cấu trúc bậc hai. Cấu trúc này bao gồm năng lực

bản thân, hiệu quả ứng phó và các rào cản được nhận thức, từ đó đo lường các khía cạnh cụ thể của nhận thức về an ninh mạng. Cấu trúc bậc hai này cho phép kết hợp ba khía cạnh khác nhau của nhận thức về an ninh mạng. Nó cung cấp một sự trình bày toàn diện và tổng thể về khái niệm, nắm bắt được bản chất nhiều mặt của nó.

Đầu tiên, năng lực bản thân là sự đánh giá về khả năng thực hiện hành vi bảo vệ của một người - liệu cá nhân đó có kỹ năng, kinh nghiệm và công cụ cần thiết để thực hiện công việc một cách có trách nhiệm hay không (Maddux & Rogers., 1983). Tương tự, khi mọi người tin vào kỹ năng của bản thân cũng như mức độ tự tin vào năng lực bản thân cao để hoàn thành mục tiêu, họ có nhiều khả năng thực hiện bước tiếp theo để hiện thực hóa mục tiêu đó. Thứ hai, hiệu quả ứng phó đánh giá hiệu quả của phản ứng thích ứng nhằm giảm thiểu mối đe dọa (Rogers., 1975). Tương tự như vậy, hiệu quả ứng phó đề cập đến sự tin tưởng của nhân viên rằng hành động được đề xuất sẽ giảm thiểu thành công mối nguy hiện có (Boss et at., 2015). Cuối cùng, các rào cản nhận thức đề cập đến sự bất tiện và chi phí mà nhân viên nhận thấy liên quan đến việc tham gia vào các hoạt động bảo vệ an ninh mạng (Li et at., 2019).

2.4. Chính sách của tổ chức và nhận thức về an ninh mạng

Chính sách của tổ chức bao gồm việc lập ra các chính sách, trách nhiệm, tiêu chuẩn và hướng dẫn để đảm bảo sử dụng an toàn và phù hợp các tài nguyên hệ thống thông tin (D'Arcy et at., 2009). Chính xác hơn, điều tra này tập trung vào việc tập trung quản trị thể chế trên các lĩnh vực cung cấp chính sách cũng như các chương trình SETA.

Đầu tiên, do có đề cương toàn diện về trách nhiệm của nhân viên và hậu quả của việc không tuân thủ, chính sách bảo mật rất có khả năng thu hút sự chú ý của nhân viên và nâng cao kiến thức của họ về các biện pháp bảo mật (Hwang et at., 2021). Tương tự như vậy, nhân viên có thể gặp khó khăn trong

việc hiểu và thực hiện các chính sách nếu chúng quá phức tạp. Hơn nữa, họ có thể gặp phải sự nhầm lẫn hoặc thiếu tự tin do không chắc chắn về hướng hành động thích hợp. Do đó, tính minh bạch của các chính sách ảnh hưởng lớn đến mức độ nhân viên tuân thủ chúng liên quan đến an ninh tổ chức (Siponen et at., 2009). Hơn nữa, việc thiếu các tiêu chuẩn bảo mật có thể góp phần gây nhầm lẫn về định nghĩa về chức năng hệ thống hiệu quả (Straub, 1990). Nguyên tắc bảo mật thông tin doanh nghiệp là thành phần cơ bản của chiến lược quản lý bảo mật hệ thống thông tin (Chan et at., 2005). Điều quan trọng là các điều tra thực nghiệm trước đây đã khẳng định mối liên hệ chặt chẽ giữa việc cung cấp chính sách và CSA (Chan et at., 2005; Hwang et at., 2021; Zwilling et at., 2022).

Thứ hai, các chương trình SETA đóng vai trò là phương tiện chính để truyền bá các hành vi có động cơ bảo vệ tại các công ty và do đó, là tiền thân có giá trị cho việc đánh giá PMT (Posey et at., 2015). Đặc biệt, các chương trình SETA sử dụng nhiều hình thức khác nhau, chẳng hạn như hội thảo, hội thảo và diễn tập, để nhấn mạnh và nâng cao kiến thức, nhận thức và năng lực về bảo mật của nhân viên. Các sự kiện này nhằm mục đích giáo dục nhân viên về kiến trúc bảo mật thông tin của công ty cũng như các chính sách, thủ tục và thực tiễn của công ty để đảm bảo tuân thủ quy định. Các chương trình này được thiết kế để trang bị cho nhân viên những thông tin và chuyên môn cần thiết để xác định rủi ro, thực hiện các hành động phòng ngừa, tuân thủ các quy tắc và thủ tục cũng như duy trì an ninh (Lee & Lee, 2002; Whitman., 2003). Tương tự, các chương trình SETA được triển khai hiệu quả có thể giáo dục nhân viên về những mối nguy hiểm mà họ gặp phải, mức độ nghiêm trọng của rủi ro bảo mật mà họ gặp phải và các phương pháp tối ưu để bảo vệ bản thân trước những rủi ro đó (Zwilling et at., 2022), từ đó tạo điều kiện cho nhận thức rộng rãi về tầm quan trọng của chính sách hệ thống thông tin (Chen et at., 2015). Về cơ bản, giáo dục an ninh đã được chứng minh là nâng cao sự hiểu

biết và sự quan tâm của nhân viên đối với vấn đề này (Siponen et at., 2009), cuối cùng là giảm hành vi rủi ro (Emin Agaoglu et at., 2009). Hơn nữa, rõ ràng là giáo dục và đào tạo có thể nâng cao năng lực của nhân viên để thực hiện nhiệm vụ của họ (Chen et at., 2015).

Hiểu biết về bảo mật thông tin là điều cần thiết để ngăn chặn vi phạm dữ liệu trong bối cảnh rủi ro và lỗ hổng ngày càng tăng (Allam et at., 2014). Các học giả cũng nhấn mạnh tác động của các chương trình SETA đối với nhận thức về an ninh mạng của nhân viên (D'Arcy et at., 2009; McCrohanet at., 2010; Posey et at., 2015; Siponen et at., 2009). Cụ thể, các chương trình SETA đã được chứng minh có mối liên hệ tích cực với tính tự tin vào năng lực bản thân (Hina et at., 2019) và hiệu quả phản hồi (Workman., 2009). Nói chung, các chương trình đào tạo nâng cao trình độ kiến thức của người tham gia về an ninh và cải thiện xu hướng hành động an toàn tại nơi làm việc của họ. Vì SETA đề cao giá trị của các quy trình an toàn đã được thiết lập nên nghiên cứu này xem xét quan điểm cho rằng những cá nhân tuân thủ quản trị của tổ chức về việc cung cấp các chính sách mà các chương trình SETA có nhiều khả năng có mức độ nhận thức cao hơn về an ninh mạng. Vì vậy, chúng tôi đề xuất các giả thuyết sau:

H1. Việc cung cấp các chính sách có liên quan tích cực đến nhận thức về an ninh mạng.

H2. Các chương trình SETA có liên quan tích cực đến nhận thức về an ninh mạng.

2.5. Nhận thức và Thái độ về an ninh mạng đối với ý định tuân thủ (ISPC)

Việc tích hợp các yếu tố cốt lõi của PMT—năng lực tự thân, hiệu quả ứng phó và các rào cản nhận thức được—cho phép đánh giá toàn diện hơn về

nhận thức an ninh mạng. Khi nhân viên hiểu được mức độ nghiêm trọng của các mối đe dọa bảo mật mà công ty họ gặp phải, họ sẽ có động lực hơn để tuân theo các biện pháp bảo mật thông tin đã được thiết lập (Siponen et at., 2009). Việc nhân viên không thực hiện các biện pháp bảo mật cơ bản là do các rào cản về bảo mật thông tin (Ng et at., 2009). Khi nhân viên tin rằng các rào cản trong việc thực thi các quy định an ninh mạng là rất lớn, họ sẽ ít có xu hướng áp dụng các biện pháp phòng ngừa hơn. Hơn nữa, nhân viên có động lực cao để tuân theo các quy định này vì họ có mức độ tự tin vào khả năng bản thân và hiệu quả ứng phó cao (Siponen et at., 2009). PMT chỉ ra rằng sự nhạy cảm có thể làm giảm bớt các phản ứng bảo vệ, chẳng hạn như đi xa hơn để đảm bảo an toàn cho bản thân (Herath & Rao., 2009; Ifinedo., 2012; Vance et at., 2012).

Nhân viên quản lý cấp cao và nhân viên bảo mật công nghệ thông tin phải ưu tiên bảo mật thông tin trong bất kỳ tổ chức nào (Safa et at., 2016). Bảo mật thông tin bao gồm các biện pháp kỹ thuật và phi -kỹ thuật. Các biện pháp kỹ thuật về bảo mật thông tin tại các tổ chức bao gồm các biện pháp phần cứng như tường lửa, phần mềm chống vi-rút, sao lưu dữ liệu, kiểm soát truy cập, mã hóa và giám sát liên tục để phát hiện các mối đe dọa (Ifinedo., 2012). Trong khi đó, các biện pháp phi kỹ thuật bao gồm hành vi của con người và tổ chức (Ifinedo., 2014). Những biện pháp này cải thiện ISPC bằng cách áp dụng các lý thuyết hành vi xã hội, tâm lý và tổ chức vào bảo mật thông tin (Ifinedo., 2014).

Đặc biệt, các điều tra thực nghiệm trước đây minh họa rằng nhận thức về các mối đe dọa trên mạng ảnh hưởng mạnh mẽ đến hành vi an ninh mạng (Alanazi et at., 2022; Dinev & Hu., 2007; Meso et at., 2013). Hướng dẫn cách tránh tổn hại nâng cao nhận thức của mọi người về các mối đe dọa có thể xảy ra (Van Bavel et at., 2019). Do đó, chúng tôi đề xuất một giả thuyết mới nghiên

cứu sâu hơn về tác động của ISPC trong việc nâng cao nhận thức cá nhân và từ đó cải thiện các EPB.

H3. CSA có liên quan tích cực đến ISPC.

2.6. Nhận thức về an ninh mạng và thái độ tuân thủ của nhân viên

Việc đảm bảo an ninh thông tin phụ thuộc rất lớn vào việc bồi dưỡng nhận thức. Cụ thể, thái độ của chúng ta đóng một vai trò then chốt trong việc ảnh hưởng đến những kích thích mà chúng ta chọn tập trung vào và những thứ chúng ta chọn bỏ qua, hoạt động như những nhân tố thiết yếu hình thành nên hành vi của con người. "Thái độ" của mọi người đề cập đến phản ứng cảm xúc của họ đối với một hành động cụ thể, phản ánh xu hướng được đào tạo để đánh giá mọi thứ theo một cách nhất định. Thái độ được hình thành bởi quan điểm, ý định và kiến thức của mọi người, những điều này ảnh hưởng chung đến quan điểm của họ về một đối tượng cụ thể. Những cá nhân có thái độ tích cực đối với một vấn đề cụ thể có xu hướng thể hiện những hành vi mang tính xây dựng liên quan đến vấn đề đó. Hơn nữa, khi các cá nhân coi một mối hiểm họa cụ thể là đáng kể, họ nhận ra sự cần thiết phải có thái độ tuân thủ để giảm thiểu rủi ro. Nhưng nếu họ không coi mối hiểm họa là có liên quan thì nhận thức về tầm quan trọng của nó sẽ thấp hơn (Hina et at., 2019; Menard et at., 2017). Tương tự, những cá nhân tin rằng họ có khả năng tránh được rủi ro sẽ ít có khả năng thực hiện các biện pháp phòng ngừa để giảm thiểu rủi ro. Do đó, nguy cơ chấn thương của họ cao hơn (Ifinedo., 2012). Về cơ bản, các chính sách được hiểu rõ hơn sau các chiến dịch nâng cao nhận thức và do đó, mọi người thường có cái nhìn tích cực hơn về việc tuân thủ các chính sách đó (Diev & Hu., 2007; Ma., 2022; Parsons et at., 2014; Williams., 2008). Do đó, chúng tôi suy đoán rằng một nhân viên có nhận thức cao hơn về tính dễ bị tổn thương sẽ thể hiện sự tuân thủ tốt hơn nhiệm vụ bảo mật. Vì vậy, giả thuyết đề xuất:

H4. CSA có quan hệ tích cực với ATT.

2.7. Thái độ tuân thủ an ninh mạng, ý định tuân thủ và hành vi bảo vệ của nhân viên

Theo TPB, thái độ của con người là động lực thúc đẩy hành động của họ (Ajzen., 1991). Cho rằng thái độ là một yếu tố dự báo mạnh mẽ về ý định, điều quan trọng là phải thực hiện nghiên cứu TPB về khía cạnh này (Bulgurcu et at., 2010; Ifinedo., 2012; Mahon et at., 2006; Zhang et at., 2009). Các cá nhân có nhiều khả năng tuân thủ luật pháp và quy định hơn nếu họ có thái độ tích cực đối với việc làm đó. Do đó, thái độ tích cực đối với ISPC hàm ý sự sẵn sàng tham gia vào các hoạt động duy trì ISPC. Tương tự như vậy, thái độ mạnh mẽ, được đánh dấu bằng mức độ tự tin và nhất quán cao, có nhiều khả năng ảnh hưởng đến hành vi hơn. Ý kiến tích cực của ISPC làm tăng đáng kể khả năng tuân thủ các quy định (Wiafe et at., 2020).

Điều tra thực nghiệm đã chỉ ra rằng việc giữ thái độ tích cực đối với các quy định ANM sẽ dẫn đến mức độ tuân thủ nhiều hơn các chuẩn mực và tiêu chuẩn liên quan đến ISPC (Bulgurcu et at., 2010; Dinev & Hu., 2007; Guo.et at., 2011; Herath & Rao., 2009; Ng.et at., 2009; Siponen et at., 2014). Ngược lại, điều này có ảnh hưởng đáng kể đến việc nhân viên áp dụng các EPB (Maalem Lahcen et at., 2020; Ng et at., 2009; Siponen et at., 2014). Do đó, chúng tôi cho rằng những cá nhân có thái độ tuân thủ an ninh mạng sẽ có thái độ tích cực đối với việc tham gia ISPC và hành vi bảo vệ. Căn cứ trên những lập luận này, giả thuyết thứ năm và thứ sáu được đề xuất:

H5. ATT có liên quan tích cực đến ISPC.

H6. ATT có liên quan tích cực đến EPB.

2.8. Ý định tuân thủ, nhận thức về an ninh mạng và hành vi bảo vệ nhân viên

Đầu tiên, ý định là một nhân tố quan trọng trong việc dự đoán hành vi vì nó tiết lộ động cơ tham gia vào hành vi đó (Armitage & Conner., 2001). Theo TPB, ý định của một cá nhân là sự thể hiện nhận thức về mục đích đi trước hành động và do đó là tiền đề trực tiếp của hành vi (Ajzen., 1985). Nói cách khác, khả năng mọi người thực hiện một hành vi mong muốn sẽ được xác nhận tùy thuộc vào sự quan tâm đến hành vi đó mà họ cảm nhận được. Tương tự, người ta giả định rằng các cá nhân thực hiện các hành động phù hợp với mục tiêu của họ khi có một cơ hội hấp dẫn và họ đánh giá chúng là những động cơ có lợi. Người ta đã chứng minh rõ ràng rằng ý định hướng tới ISPC đóng vai trò quyết định hành vi bảo vệ của nhân viên (Swaim et at., 2014).

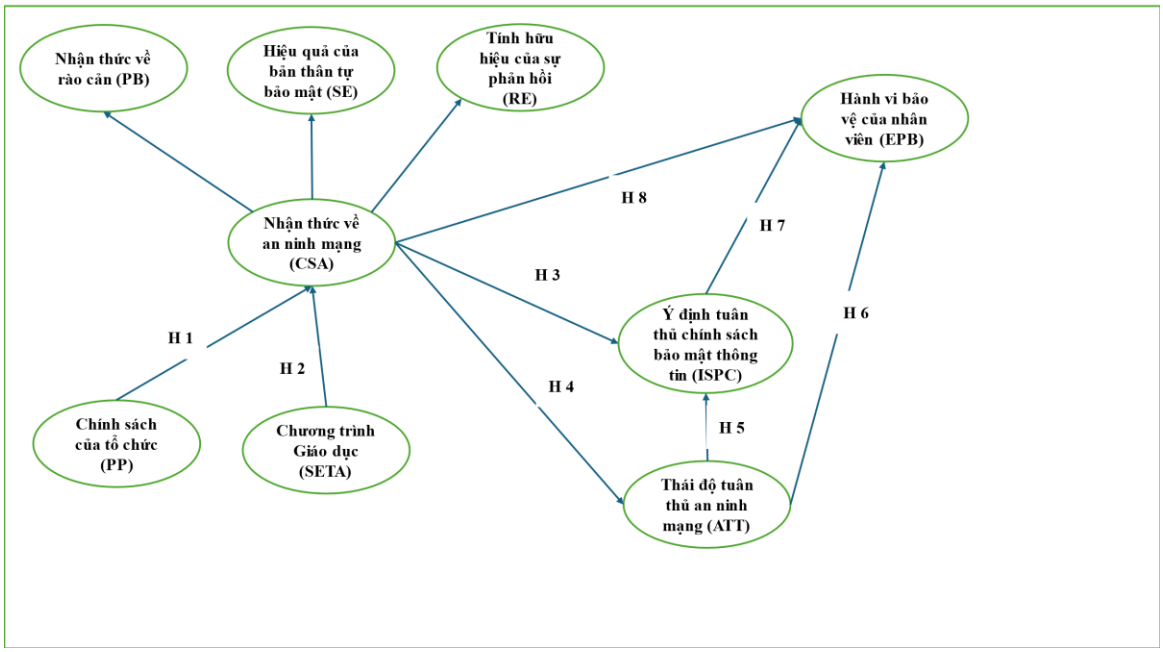
Thứ hai, nhân viên cần được thông báo về những rủi ro trong thế giới mạng để họ có thể thực hiện các biện pháp bảo vệ bản thân và công ty của mình. Nhân viên ít có khả năng thực hiện các quy trình an ninh mạng một cách nhiệt tình nếu họ nhận thấy những rào cản đáng kể (Ng & Xu., 2007). Họ trở nên thận trọng hơn trước những hành vi tiềm ẩn rủi ro có thể gây nguy hiểm cho an ninh doanh nghiệp. Hơn nữa, họ có xu hướng thực hiện các biện pháp phòng ngừa an toàn hơn nếu họ tin rằng họ có kỹ năng ứng phó thành công với bất kỳ tình huống nào (Johnston & Warkentin., 2010). Ý thức tự chủ cao về an ninh mạng có nghĩa là nhân viên tự tin về khả năng thực hiện các biện pháp bảo mật bổ sung của họ. Nói cách khác, họ có xu hướng thực hành nhận thức về an toàn và các biện pháp phòng ngừa nhiều hơn. Do đó, nhân viên có nhiều khả năng tuân thủ các chính sách bảo mật thông tin hơn nếu họ nhận thức được khả năng và hậu quả của việc không tuân thủ các chính sách đó (Tsohou et at., 2015). Điều tra trước đây chứng minh rằng nhận thức về an ninh mạng ảnh hưởng mạnh mẽ đến hành vi an ninh mạng (Lee & Kim., 2023; Li et at., 2016, 2022). Cuối cùng, dựa trên cuộc thảo luận trước đó, chúng tôi

cho rằng những nhân viên có ý định tuân thủ các chính sách bảo mật thông tin có nhiều khả năng nhận thức được các rủi ro an ninh mạng hơn, dẫn đến việc thực hiện các biện pháp phòng ngừa. Vì vậy, giả thuyết thứ bảy và thứ tám được đặt ra:

H7. ISPC có liên quan tích cực đến EPB.

H8. CSA có liên quan tích cực đến EPB.

Hình 3.1 mô tả mô hình nghiên cứu của chúng tôi, bao gồm 08 giả thuyết về việc kết hợp IG với PMT và TPB. Trong mô hình, nhận thức về an ninh mạng là cấu trúc bậc hai bao gồm ba cấu trúc bậc nhất: rào cản nhận thức, tính tự tin vào năng lực bản thân và hiệu quả phản hồi. Qua thiết lập nhận thức về an ninh mạng như một cấu trúc bậc hai, nghiên cứu trước đây được thảo luận trong tổng quan tài liệu.



Hình 3.1. Mô hình nghiên cứu

Nguồn: Tác giả xây dựng

3. Phương pháp nghiên cứu

3.1. Thang đo

Công cụ khảo sát trong bài viết này được phát triển dựa trên tài liệu hiện có. Các mục câu hỏi được đánh giá bằng thang đo Likert bảy điểm, từ 1 (rất không đồng ý) đến 7 (rất đồng ý). Các thang đo được sử dụng để đo lường được điều chỉnh từ điều tra trước đó. Đặc biệt, việc cung cấp các chính sách và chương trình SETA được đo lường bằng thang đo được điều chỉnh từ các điều tra trước đó (Haeussinger & Kranz, 201); Hina et at., 2019) và ý định hướng tới ISPC được đo lường bằng thang đo được điều chỉnh từ các điều tra trước đó (Hina et at., 2019; Ifinedo, 2012). Để đo lường nhận thức về an ninh mạng, mức độ tự tin vào năng lực bản thân đã được điều chỉnh bằng thang đo bảy mục từ điều tra trước đó (Hina et at., 2019; Ifinedo., 2014; Li et at., 2019), hiệu quả ứng phó đã được điều chỉnh theo thang đo mười mục từ các điều tra trước đây (Hina et at., 2019; Ifinedo., 2012; Li et at., 2019; Vance et at., 2012; Wong et at., 2022), và các rào cản nhận thức được điều chỉnh từ Li et at. (2019). Thái độ được đo lường bằng thang đo ba mục được điều chỉnh từ Hina et at. (2019) và Ifinedo. (2014). Cuối cùng, EPB đã được điều chỉnh theo thang đo ba mục từ Li et at. (2019).

Bảng 3.1 các hạng mục đo lường.

Xây dựng (Nguồn)	Số biến	Hạng mục đo lường	Sửa đổi
Chính sách tổ chức (Hina et at., 2019)	PP1	Tôi nhận thấy sự bất tiện khi phải thường xuyên kiểm tra tính bảo mật của một email có file đính kèm.	Sửa đổi nhỏ
	PP2	Tôi nhận thấy việc thường xuyên phải thay đổi cài đặt quyền riêng tư trên các trang mạng xã hội là một điều bất tiện.	Sửa đổi nhỏ

	PP3	Tôi nhận thấy việc thường xuyên sao lưu dữ liệu trên máy tính là một việc rất bất tiện.	Sửa đổi nhỏ
	PP4	Tôi nhận thấy sự bất tiện khi phải thường xuyên kiểm tra tính bảo mật của một email có file đính kèm.	Sửa đổi nhỏ
Chính sách tổ chức: Chương trình giáo dục (Hina et at., 2019)	SETA1	Tổ chức của tôi định kỳ tóm tắt về các vấn đề vi phạm an toàn thông tin để nâng cao nhận thức thông qua e-mail, brochure / hội thảo / hội thảo.	Sửa đổi nhỏ
	SETA2	Tổ chức của tôi cập nhật cho tôi về các vi phạm an toàn thông tin *(an ninh mạng)* và các biện pháp ngăn chặn.	Sửa đổi nhỏ
	SETA3	Tổ chức của tôi tiếp tục giáo dục nhân viên về trách nhiệm tự bảo mật máy tính *(an ninh mạng)* của họ.	Sửa đổi nhỏ
	SETA4	Các chương trình đào tạo về bảo mật thông tin của tổ chức tôi cung cấp cho tôi thông tin đầy đủ về các mối đe dọa về bảo mật.	Sửa đổi nhỏ
	SETA5	Các chương trình nâng cao nhận thức về an toàn thông tin *(an ninh mạng)* của tổ chức tôi giúp nhân viên phát triển các kỹ năng cần thiết, để áp dụng hành vi bảo vệ.	Sửa đổi nhỏ
Nhận thức về ANM PMT: Nhận thức về an ninh mạng (CSA) (Bulgurcu, et al., 2010)	GCA1	Nhìn chung, tôi nhận thức được các mối đe dọa về bảo mật *(an ninh mạng)* an toàn thông tin và hậu quả tiêu cực của chúng.	Sửa đổi nhỏ
	GCA2	Tôi có đủ kiến thức nhận biết về hậu quả của việc thông tin (an ninh mạng) bị mất cắp.	Sửa đổi nhỏ
	GCA3	Tôi hiểu những lo ngại về an ninh mạng liên quan đến bảo mật thông tin và những rủi ro khi thông tin bị mất cắp.	Sửa đổi nhỏ
Nhận thức về ANM PMT:	SE1	Tôi tin rằng tôi có các kỹ năng cần thiết để tự bảo vệ mình khỏi các hành vi vi phạm an toàn thông tin *(an ninh mạng)*.	Sửa đổi nhỏ

Hiệu quả của bản thân tự bảo mật (Hina et at., 2019; Li et at., 2022)	SE2	Tôi tin rằng tôi đã phát triển khả năng ngăn chặn mọi người lấy cắp thông tin bí mật của tôi.	Sửa đổi nhỏ
	SE3	Tôi bật các biện pháp bảo mật *(tường lửa, chống vi-rút, v.v.)* trên tài nguyên máy tính công việc của mình.	Sửa đổi nhỏ
	SE4	Tôi tin rằng việc tự bảo vệ mình khỏi các hành vi vi phạm bảo mật an toàn thông tin *(an ninh mạng)*, nằm trong tầm kiểm soát của tôi.	Sửa đổi nhỏ
	SE5	Tôi tự tin khi mở duyệt trình web ở các mức độ bảo mật khác nhau.	Sửa đổi nhỏ
	SE6	Tôi cảm thấy tự tin khi xử lý các file bị nhiễm virus.	Sửa đổi nhỏ
	SE7	Tôi cảm thấy tự tin khi loại bỏ các phần mềm gián điệp và phần mềm độc hại khỏi máy tính.	Sửa đổi nhỏ
Nhận thức về ANM PMT: Hiệu quả đáp ứng (Hina et at., 2019; Li et at., 2019; Wong et at., 2022)	RE1	Trong tổ chức của tôi, những nỗ lực để đảm bảo an toàn thông tin *(an ninh mạng)*, bí mật của tôi là có hiệu quả.	Sửa đổi nhỏ
	RE2	Tại tổ chức của tôi, các biện pháp bảo mật *(an ninh mạng)* hiện có để bảo vệ an toàn thông tin, công việc của tôi khỏi các vi phạm bảo mật *(an ninh mạng)* đều có hiệu lực.	Sửa đổi nhỏ
	RE3	Các biện pháp phòng ngừa an ninh mạng có sẵn cho tôi tại tổ chức của tôi, để đối phó với nội dung độc hại, đều có hiệu quả.	Sửa đổi nhỏ
	RE4	Các biện pháp bảo mật an toàn thông tin *(an ninh mạng)* tại tổ chức của tôi đã ngăn chặn tin tặc truy cập vào thông tin cá nhân hoặc giáo dục nhạy cảm.	Sửa đổi nhỏ
	RE5	Việc tuân thủ các chính sách bảo mật an toàn thông tin trong tổ chức sẽ ngăn chặn các vi phạm bảo mật an toàn thông tin, an ninh mạng.	Sửa đổi nhỏ

	RE6	Nếu tôi tuân thủ các chính sách bảo mật thông tin *(an ninh mạng)*, khả năng xảy ra vi phạm an toàn thông tin *(an ninh mạng)* sẽ giảm xuống.	Sửa đổi nhỏ
	RE7	Tuân thủ cẩn thận các chính sách bảo mật thông tin giúp tránh các vấn đề về an ninh mạng.	Sửa nhỏ
	RE8	Tổ chức có thể cải thiện an toàn thông tin *(an ninh mạng)* khi người dùng chỉ ra được sơ suất về bảo mật *(an ninh mạng)* của họ đến tình hình an ninh mạng của tổ chức.	Sửa đổi nhỏ
	RE9	Tổ chức nên có Quy định chung về Bảo vệ Dữ liệu *(an ninh mạng).*	Sửa đổi nhỏ
	RE10	Tổ chức nên thường xuyên nâng cấp phần mềm chống virus và tường lửa.	Sửa đổi nhỏ
Nhận thức về ANM PMT: nhận thức về rào cản (Li et at., 2019)	PB1	Tôi nhận thấy sự bất tiện khi phải thường xuyên kiểm tra tính bảo mật của một email có file đính kèm.	Sửa đổi nhỏ
	PB2	Tôi nhận thấy việc thường xuyên phải thay đổi cài đặt quyền riêng tư trên các trang mạng xã hội là một điều bất tiện.	Sửa đổi nhỏ
	PB3	Tôi nhận thấy việc thường xuyên sao lưu dữ liệu trên máy tính là một việc rất bất tiện.	Sửa đổi nhỏ
Hành vi bảo vệ của nhân viên (Li et at., 2019)	EPB1	Tôi luôn cập nhật phần mềm chống vi-rút trên máy tính của mình.	Sửa đổi nhỏ
	EPB2	Tôi theo dõi các dấu hiệu bất thường của máy tính (ví dụ: máy tính chạy chậm hoặc bị treo, nhiều cửa sổ bật lên, v.v.).	Sửa đổi nhỏ
	EPB3	Tôi luôn quan tâm bất kỳ phần mềm độc hại nào được cảnh báo qua các kênh thông tin truyền thông.	Sửa đổi nhỏ
Thái độ tuân thủ an ninh	ATT1	Tôi có ý định thực hiện việc bảo vệ các nguồn thông tin và công nghệ theo các yêu cầu của	Sửa đổi nhỏ

mạng (Hina., 2019)		Chính sách An toàn Thông tin *(an ninh mạng)* của tổ chức.	
	ATT2	Tôi có ý định tuân thủ các yêu cầu của Chính sách Bảo mật Thông tin *(an ninh mạng)* của tổ chức.	Sửa đổi nhỏ
	ATT3	Tôi có ý định thực hiện các trách nhiệm của mình đối với Chính sách Bảo mật Thông tin *(an ninh mạng)*.	Sửa đổi nhỏ
Ý định về việc tuân thủ (ISPC) (Hina et at., 201	ISPC1	Tôi có ý định thực hiện việc bảo vệ các nguồn thông tin và công nghệ theo các yêu cầu của Chính sách An toàn Thông tin *(an ninh mạng)* của tổ chức.	Sửa đổi nhỏ
	ISPC2	Tôi có ý định tuân thủ các yêu cầu của Chính sách Bảo mật Thông tin *(an ninh mạng)* của tổ chức.	Sửa đổi nhỏ
	ISPC3	Tôi có ý định thực hiện các trách nhiệm của mình đối với Chính sách Bảo mật Thông tin *(an ninh mạng)*.	Sửa đổi nhỏ
	ISPC4	Tôi có ý định tiếp tục tuân thủ Chính sách Bảo mật Thông tin của tổ chức.	Sửa đổi nhỏ

3.2. Thu thập dữ liệu

Từ tháng 10 năm 2022 đến tháng 4 năm 2023, các mẫu khảo sát tự thực hiện được phân phát cho nhiều nhóm nhân viên khác nhau tại công ty ở các khu vực thành thị và tỉnh lớn ở Việt Nam. Chúng tôi đã phân phát tổng cộng 750 bảng câu hỏi, trong đó có 594 bảng được trả lại, với tỷ lệ phản hồi là 79,2% và trong số đó.

Trong tổng số các mẫu hỏi được thu về, 323 mẫu hỏi được xem là phù hợp để đưa vào điều tra. Sự phù hợp của cỡ mẫu được xác định dựa trên điều tra được thực hiện bởi Hair et at. (2014). Các bảng câu hỏi không đáp ứng bất kỳ tiêu chuẩn nào sau đây được xem là không hợp lệ và sau đó bị loại bỏ. Hai

điều kiện có thể chỉ ra các vấn đề tiềm ẩn với dữ liệu khảo sát: thứ nhất, nếu người trả lời đưa ra tất cả câu trả lời giống nhau cho tất cả các câu hỏi, chẳng hạn như chọn tùy chọn xếp hạng thấp nhất hoặc cao nhất cho từng mục; thứ hai, nếu người trả lời hoàn thành bảng câu hỏi trong vòng chưa đầy hai phút, như Collier & Sherrell (2009) đã xác định.

Nghiên cứu này sử dụng *t* -test để đánh giá các đặc điểm nhân khẩu học của những người trả lời ban đầu và cuối cùng, theo khuyến nghị của các nghiên cứu trước đây, nhằm giảm thiểu bất kỳ sai lệch tiềm ẩn nào khi không phản hồi (Collier & Sherrell, 2009; Han et at., 2017). Do không có sự khác biệt có thể quan sát được giữa hai nhóm người tham gia, nên xu hướng không phản hồi dường như không gây ra mối lo ngại đáng kể. Bảng 3.2 cung cấp cái nhìn tổng quan về thông tin cơ bản về người trả lời và công ty tương ứng của họ.

Bảng 3.2. Đặc điểm chính của người trả lời

Đặc điểm dân số	Loại	*N* = 323	Tỷ lệ (%)
Giới tính	Nam	217	67,18
	Nữ giới	106	32,82
	18-30 tuổi	52	16,10
Tuổi	31-40	184	56,97
	Hơn 40 năm	87	26,93
	Trung học phổ thông	66	20,43
Trình độ học vấn	Đại học	187	57,89
	Sau đại học	70	21,67
	Dưới 3 năm	49	15.17
Số năm kinh nghiệm	Từ 3 đến 5 năm	67	20,74
	Trên 5 năm	207	64,09
	Dưới 50 nhân viên	97	30,03

Quy mô tổ chức	Từ 51 đến 100 nhân viên	68	21,05
	Trên 100 nhân viên	158	48,92

Nguồn: Được tạo bởi các tác giả.

4. Kết quả

PLS-SEM được áp dụng để phân tích các câu hỏi điều tra bằng cách kiểm tra mối quan hệ giữa các biến phụ thuộc, trung gian và độc lập. Khi nhận xét mối liên hệ giữa các biến, PLS-SEM xem xét độ chính xác của phép đo và mức độ dữ liệu phù hợp với mô hình khái niệm.

4.1 Đánh giá mô hình đo lường

R 2 cho biết mẫu dự đoán các biến nội sinh tốt đến mức nào. Giá trị ngưỡng chấp nhận được là 0,13 và giá trị cao là 0,26 (Hair et at., 2019). *R 2* về nhận thức an ninh mạng, thái độ tuân thủ an ninh mạng, ý định đối với ISPC và hành vi bảo vệ nhân viên lần lượt là 0,636, 0,162, 0,570 và 0,468. Vì vậy, kết quả là thỏa đáng.

Bảng 3.3 cho thấy các hệ số tới hạn để đánh giá độ hội tụ và giá trị phân biệt. Đầu tiên, hệ số tải của các biến đo lường được tính toán để đánh giá tính hợp lệ hội tụ. Độ giá trị hội tụ được thỏa mãn vì điểm tải nhân tố của từng mục đều lớn hơn ngưỡng 0,5 (Hair et at., 2010). Thứ hai, Cronbach's alpha là một thống kê dùng để đánh giá độ tin cậy và giá trị của một công cụ đo lường. Các hệ số cho mỗi cấu trúc vượt quá tiêu chí 0,6 (Hair et at., 2010). Tiếp theo, các giá trị độ tin cậy tổng hợp (CR) nằm trên ngưỡng 0,70, cho thấy mô hình đo lường là đáng tin cậy và nhất quán. Cuối cùng, phương sai trích trung bình (AVE) được sử dụng để đánh giá giá trị phân biệt. Đặc biệt, giá trị phân biệt của các cấu trúc được xác nhận vì giá trị AVE nằm trên ngưỡng 0,5 (Hair et at., 2010).

Bảng 3.3. Đánh giá đo lường

Cấu trúc	Ký hiệu	**Hệ số tải (>0.5)**	Alpha **(α>0.7)**	**CR (>0.7)**	**AVE (>0.5)**	**FCVIF (<3.3)**
Chính sách của tổ chức (PP)	PP1	0.890	0.925	0.927	0.817	3.033
	PP2	0.933				
	PP3	0.871				
	PP4	0.920				
Chương trình Giáo dục (SETA)	SETA1	0.927	0.959	0.960	0.858	3.099
	SETA2	0.931				
	SETA3	0.943				
	SETA4	0.928				
	SETA5	0.903				
Nhận thức về an ninh mạng (CSA)						
Tính hữu hiệu của sự phản hồi (RE)	RE1	0.860	0.939	0.960	0.648	1.480
	RE2	0.848				
	RE3	0.825				
	RE4	0.813				
	RE5	0.793				
	RE6	0.812				
	RE7	0.803				
	RE8	0.842				
	RE9	0.737				
	RE10	0.704				
Hiệu quả của bản thân tự bảo mật (SE)	SE1	0.846	0.942	0.944	0.744	1.944
	SE2	0.898				
	SE3	0.825				

	SE4	0.895				
	SE5	0.910				
	SE6	0.824				
	SE7	0.834				
Nhận thức về rào cản (PB)	PB1	0.753	0.830	1.177	0.683	1.045
	PB2	0.742				
	PB3	0.965				
Ý định tuân thủ chính sách bảo mật thông tin (ISPC)	ISPC1	0.879	0.932	0.934	0.832	1.542
	ISPC2	0.924				
	ISPC3	0.939				
	ISPC4	0.905				
Thái độ tuân thủ an ninh mạng (ATT)	ATT1	0.893	0.883	0.884	0.810	1.334
	ATT2	0.911				
	ATT3	0.869				
Hành vi bảo vệ của nhân viên (EPB)	EPB1	0.915	0.914	0.925	0.854	1.140
	EPB2	0.940				
	EPB3	0.916				

Nguồn: Được tạo bởi các tác giả.

Tiêu chí Fornell và Larcker và tỷ lệ tính trạng dị tính (HTMT) được đánh giá để thiết lập giá trị phân biệt. Giá trị phân biệt đối xử khi sử dụng HTMT phải có giá trị nhỏ hơn 0,90 cho mối tương quan giữa các cấu trúc để chứng minh sự vắng mặt của vấn đề phân biệt đối xử (Henseler et at., 2015). Bảng 3 minh họa rằng tất cả các chỉ số của các cấu trúc được tạo ra đều nhỏ hơn 0,9. Hơn nữa, bằng cách sử dụng căn bậc hai của AVE, như Fornell và Larcker đề xuất, chúng tôi xác nhận giá trị phân biệt đối xử của công cụ (Fornell and Larcker, 1981). Bảng 3.4 cho thấy căn bậc hai của AVE có giá trị

phân biệt cao hơn bất kỳ thành phần nào khác, do đó nó biểu thị giá trị phân biệt thỏa đáng.

4.2 Độ lệch phương pháp phổ biến

Một số học giả đã phát hiện ra rằng cộng tuyến hoàn toàn có thể được sử dụng để phát hiện sai lệch phương pháp chung (CMB). Theo Kock (2015), nếu giá trị cộng tuyến đầy đủ (FCVIF) dưới 3,3 thì dữ liệu không có mối lo ngại liên quan đến cộng tuyến. Bảng 3.4 chứng minh rằng tất cả các cấu trúc tiềm ẩn trong dữ liệu đều có giá trị FCVIF nhỏ hơn 3,3, biểu thị rằng không có vấn đề về CMB.

Bảng 3.4. Giá trị phân biệt (*Tỷ lệ HTMT và tiêu chí Fornell-Larcker*)

Cấu trúc	ATT	EPB	ISPC	PB	PP	RE	SETA	SE
Tỷ lệ HTMT								
Thái độ tuân thủ an ninh mạng (ATT)								
Hành vi bảo vệ của nhân viên (EPB)	0.467							
Ý định tuân thủ chính sách bảo mật thông tin (ISPC)	0.540	0.726						
Nhận thức về rào cản (PB)	0.031	0.030	0.055					
Chính sách của tổ chức (PP)	0.487	0.743	0.733	0.063				
Tính hữu hiệu của sự phản hồi (RE)	0.495	0.733	0.779	0.072	0.809			
Chương trình giáo dục (SETA)	0.378	0.730	0.714	0.073	0.889	0.774		
Hiệu quả của bản thân tự bảo mật (SE)	0.303	0.720	0.646	0.070	0.682	0.798	0.743	
Tiêu chí Fornell-Larcker								
Cấu trúc	ATT	EPB	ISPC	PB	PP	RE	SETA	SE
Thái độ tuân thủ an ninh mạng (ATT)	**0.900**							
Hành vi bảo vệ của nhân viên (EPB)	0.425	**0.924**						

Ý định tuân thủ chính sách bảo mật thông tin (ISPC)	0.491	0.676	**0.912**					
Nhận thức rào cản (PB)	-0.016	-0.007	-0.021	**0.826**				
Chính sách của tổ chức (PP)	0.441	0.683	0.682	-0.058	**0.904**			
Tính hữu hiệu của sự phản hồi (RE)	0.449	0.689	0.731	-0.037	0.760	**0.805**		
Chương trình giáo dục (SETA)	0.348	0.682	0.675	-0.068	0.840	0.745	**0.926**	
Hiệu quả của bản thân tự bảo mật (SE)	0.282	0.666	0.608	-0.079	0.638	0.763	0.707	**0.863**

Lưu ý: Căn bậc hai của AVE được in đậm trên đường chéo.
Nguồn: Được tạo bởi các tác giả.

Kết quả kiểm định giả thuyết được trình bày ở Bảng 3.5. Kết quả 8 giả thuyết đều được chấp nhận ở mức độ đáng kể. Ngoài ra, các tác động gián tiếp được ước tính để xác định tác động trung gian của ISPC và ATT đối với mối quan hệ giữa CSA, ISPC, ATT và hành vi bảo vệ nhân viên. Do đó, Bảng 3.6 minh họa rằng ATT làm trung gian hòa giải một phần cho mối liên hệ giữa CSA và ISPC. Hơn nữa, ISPC làm trung gian hòa giải một phần cho mối quan hệ giữa ATT và EPB cũng như CSA và EPB.

Bảng 3.5. Kết quả kiểm định giả thuyết

Giả thuyết	*P*	Giá trị t	Giá trị p	Kết quả
H1. PP → CSA	0,348	3.182	0,001	Chấp nhận
H2. CSA → CSA	0,483	4.755	0,000	Chấp nhận
H3. CSA → ISPC	0,722	13,780	0,000	Chấp nhận
H4. CSA → ATT	0,403	4.852	0,000	Chấp nhận
H5. ATT → ISPC	0,239	3.274	0,001	Chấp nhận
H6. ATT → EPB	0,270	3.673	0,000	Chấp nhận

H7. ISPC → EPB	0,616	8.080	0,000	Chấp nhận
H8. CSA → EPB	0,494	4.852	0,000	Chấp nhận

Nguồn: Được tạo bởi các tác giả.

Bảng 3.6. Hiệu ứng trung gian

Giả thuyết	Kiểu	Ước lượng	Giá trị T	Giá trị p	Bình luận
H3. CSA → ISPC	Trực tiếp	0,722	13,780	0,000	Chấp nhận
CSA →ATT → ISPC	gián tiếp	0,096	2.411	0,016	Bổ sung (một phần)
H6. ATT → EPB	Trực tiếp	0,270	3.673	0,000	Chấp nhận
ATT → ISPC → EPB	gián tiếp	0,147	3,547	0,000	Bổ sung (một phần)
H8. CSA → EPB	Trực tiếp	0,494	4.852	0,000	Chấp nhận
CSA → ISPC → EPB	gián tiếp	0,386	4.575	0,000	Bổ sung (một phần)

Nguồn: Được tạo bởi các tác giả.

5. Thảo luận

Điều tra này nâng cao sự hiểu biết về các nhân tố góp phần hình thành ISPC và EPB tại doanh nghiệp bằng cách tạo ra và đánh giá mô hình điều tra kết hợp hai khung lý thuyết hiện tại. Nó bổ sung vào tài liệu về ANM bằng cách tạo ra một khung khái niệm để thúc đẩy các thực hành an toàn mạng tại nơi làm việc và giải quyết lỗ hổng kiến thức bằng cách tích hợp TPB và PMT trong khung lý thuyết. Những người thực hành có thể sử dụng những khám phá của chúng tôi để củng cố nỗ lực khuyến khích nhân viên tuân thủ các quy trình an toàn.

5.1. Quản trị thể chế trong việc nâng cao nhận thức về an ninh mạng

Phát hiện của chúng tôi được xây dựng dựa trên kiến thức hiện tại bằng cách nêu bật tầm quan trọng của quản trị thể chế hiệu quả trong việc nâng cao CSA của nhân viên. Kết quả chỉ ra rằng việc thực hiện các quy định được thiết kế tốt có thể nâng cao hiểu biết của người dân về các mối lo ngại về ANM, hàm ý rằng các luật hiệu quả có thể nâng cao nhận thức về các mối đe dọa này. Mục tiêu chính là đảm bảo rằng nhân viên có kiến thức và sự tự tin cần thiết để thực hiện những điều này.

Các biện pháp an ninh và tin chắc rằng việc chấp hành các tiêu chuẩn này sẽ giúp ngăn chặn các vi phạm an ninh. Kết quả này phù hợp với những phát hiện trong các điều tra trước đây về tác động của chính sách đối với CSA (Chan et at., 2005; Hwang et at., 2021; Zwilling et at., 2022). Tương tự, những khám phá của chúng tôi chứng minh mối quan hệ rõ ràng giữa các chương trình SETA với kiến thức và hiểu biết ngày càng tăng về ANM. Nhân viên có nhiều khả năng áp dụng các biện pháp phòng ngừa an toàn hơn nếu họ có hiểu biết và nhận thức toàn diện về những thách thức liên quan đến việc xác định các trường hợp sử dụng sai mục đích. Phát hiện này cũng phù hợp với những khám phá trong các điều tra trước đây (D'Arcy et at., 2009; McCrohan et at., 2010; Posey et at., 2015; Siponen et at., 2009).

5.2. Tầm quan trọng của việc tuân thủ an ninh thông tin trong việc thúc đẩy hành vi bảo vệ nhân viên

Theo những phát hiện trước đây về bảo mật thông tin, nhận thức rõ ràng về tầm quan trọng của việc tuân thủ, ý định bảo mật và thái độ là rất quan trọng. Như đã chỉ ra trong điều tra trước đây, CSA và ý định hướng tới ISPC có mối tương quan chặt chẽ với nhau (Alanazi et at., 2022; Bauer & Bernroider., 2017; Dinev & Hu., 2007; Meso et at., 2013; Van Bavel et at., 2019), CSA tác động đáng kể đến EPB (Lee & Kim., 2023; Li et at., 2016,

2022). Ngoài ra, CSA có liên quan tích cực đến ATT, điều này nhất quán với các điều tra trước đây (Bin-Abbas & Bakry., 2014; Dinev & Hu, 2007; Handford et at., 2015; Ma., 2022; Parsons et at., 2014; William., 2008). Vì vậy, các nhà quản lý bắt buộc phải nhận thức được tầm quan trọng của việc ý định tuân thủ ISPC của nhân viên.

Kết quả của điều tra này chứng minh mối tương quan giữa sự gắn bó và thái độ liên quan đến ý định tuân thủ ISPC, phù hợp với điều tra trước đó (Dilev & Hu., 2007; Guo et at., 2011; Herath & Rao., 2009; Siponen et at., 2014; Swaim et at., 2014), an ninh mang ATT hình thành EPB (Maalem Lahcen et at., 2020; Ng et at., 2009; Siponen et at., 2014). Tương tự, ý định tuân thủ ISPC có tác động tích cực và đáng kể đến EPB, phù hợp với những phát hiện trước đó (Swaim et at., 2014). Mức độ dự định và khả năng tuân thủ có liên quan trực tiếp. Nhiều nền văn hóa tổ chức có thể khen ngợi những nguyên tắc quan trọng mà tất cả nhân viên phải tuân theo mà không đánh giá mức độ sẵn sàng hoặc cam kết của họ đối với những ý tưởng này. Khi mọi người hiểu được lý do của một hoạt động, họ sẽ có nhiều nỗ lực hơn để thực hiện nó. Hầu hết nhân viên không có đủ năng lực trong lĩnh vực của mình do không được đào tạo về ANM, dẫn đến thiếu hiểu biết và thừa nhận những khó khăn trong việc thực hiện các dự án ANM bền vững. Vì vậy, các tổ chức cần cải thiện chiến lược hiểu biết và dự đoán hành động của mọi người khi họ có ý định hành vi mạnh mẽ hơn.

5.3. Hiệu ứng trung gian

Các kết quả về việc điều chỉnh một phần ATT an ninh mạng cung cấp những hiểu biết sâu sắc về hành vi bằng cách nhấn mạnh ảnh hưởng của ATT đối với ISPC. Đầu tiên, họ nhấn mạnh rằng quan điểm và thái độ của cá nhân đối với các hoạt động ANM là rất quan trọng để biến nhận thức thành ý định hành vi cụ thể về việc tuân thủ các PP bảo mật thông tin. Thứ hai, kết quả

ISPC là người hòa giải một phần ngụ ý rằng ý định của nhân viên, bị ảnh hưởng bởi thái độ của họ, đóng một vai trò quan trọng trong việc xác định các EPB bảo vệ mà họ thể hiện ở nơi làm việc.

6. Đóng góp về mặt lý luận và thực tiễn

6.1. Đóng góp lý thuyết

Mục tiêu chính của nghiên cứu này là tăng cường ISPC bằng cách kết hợp chuyên môn bảo mật, nâng cao nhận thức về an ninh mạng và khuyến khích tư duy tập trung vào tuân thủ để nâng cao năng lực của nhân viên.

Hành vi bảo vệ chống lại các cuộc tấn công tiềm năng. Nghiên cứu này tập trung vào việc cung cấp PP và các chương trình SETA trong tài liệu về ANM, lấp đầy khoảng trống đáng chú ý. Cấu trúc này được mở rộng và phù hợp với các tổ chức ở các nước đang phát triển. Điều tra sử dụng một phương pháp độc đáo bằng cách kết hợp PMT và TPB để khám phá mối liên hệ giữa nhận thức, thái độ, ý định và hành vi. Nóđánh giá quản trị thể chế trong lĩnh vực ANM. Điều tra này đóng góp quan trọng về mặt khoa học cho việc phát triển kế hoạch chiến lược ANM bằng cách tích hợp các phương pháp thành công và đề xuất các cải tiến trong hoạt động phòng ngừa của nhân viên. Do đó, nó nhấn mạnh tầm quan trọng cho các nhà quản lý an ninh trong việc tích hợp các PP và tài nguyên bảo mật vào văn hóa nơi làm việc để thúc đẩy các EPB an toàn của nhân viên.

6.2. Hàm ý quản trị

Kết quả điều tra của chúng tôi có ảnh hưởng đáng kể tới các chuyên gia trong ngành bảo mật thông tin. Đầu tiên, cần có một khuôn khổ quản trị thể chế hiệu quả, cần hỗ trợ sự tham gia của nhân viên vào các hoạt động ANM. Nhà quản lý phải tạo và phổ biến các hướng dẫn, giao thức và điểm chuẩn toàn diện cho tất cả các khía cạnh của ANM. Điều này giúp nhân viên hiểu được

nhiệm vụ của mình trong việc bảo vệ thông tin bí mật. Các nhà quản lý chiến lược nên tiến hành một chiến dịch giáo dục kỹ lưỡng để nâng cao sự hiểu biết của tổ chức về các khái niệm bảo mật này. Các sự kiện bảo mật đã được tiết lộ ra bên ngoài tổ chức nên được thảo luận trong các cuộc họp và buổi đào tạo nhân viên. Những cá nhân thể hiện sự cống hiến mạnh mẽ trong việc tuân thủ các tiêu chuẩn bảo mật thông tin cần được ghi nhận vì những nỗ lực của họ.

Thứ hai, các nhà quản lý an ninh mạng nên sắp xếp các chương trình đào tạo và nâng cao nhận thức để hướng dẫn nhân viên về các quy trình bảo mật của công ty. Các tổ chức nên coi SETA như một động lực và nhấn mạnh tầm quan trọng của việc cảnh giác trước những nguy hiểm có thể xảy ra. Chương trình đào tạo phải chứa các ví dụ về vi phạm bảo mật tại các tổ chức khác do cài đặt phần mềm "miễn phí", cùng với các tình huống khác nhau bao gồm tất cả các lĩnh vực của nhà cung cấp dịch vụ Internet (ISPC). Các tổ chức nên khuyến khích trao đổi kiến thức và kinh nghiệm về xử lý rủi ro mạng và ngăn ngừa các mối đe dọa. Người quản lý có thể khuyến khích nhân viên chia sẻ kiến thức về bảo mật thông tin bằng các biện pháp khuyến khích nội bộ và bên ngoài.

Cuối cùng, điều cần thiết là nhân viên phải hiểu các mối đe dọa mạng tiềm ẩn như một phần của việc quản lý bảo mật thông tin thành công. Quản lý bảo mật cần nêu bật những lợi ích của ISPC đối với khách hàng và tổ chức, đồng thời nhấn mạnh những hạn chế của việc không tuân thủ. Phần thưởng bằng tiền, sự thừa nhận của công chúng và cơ hội thăng tiến nghề nghiệp có thể truyền cảm hứng cho các cá nhân tham gia vào các hoạt động liên quan đến an ninh mong muốn. Quản lý cấp cao nên tham gia vào việc lập kế hoạch chiến lược để thuyết phục nhân viên rằng những lo ngại về an ninh thông tin là có thật và có khả năng gây tổn hại đáng kể cho công ty. Nhận thức về bảo mật thông tin đòi hỏi phải sửa đổi liên tục trong các chiến dịch nâng cao nhận thức để thích ứng với những rủi ro và mối đe dọa ngày càng gia tăng. Việc

tích hợp đầy đủ các sáng kiến nâng cao nhận thức vào văn hóa công ty là điều cần thiết để đảm bảo rằng nhân viên được cung cấp đầy đủ thông tin. Việc đào tạo nâng cao nhận thức về an toàn thông tin hiệu quả phụ thuộc vào tính phù hợp và nhất quán của khóa đào tạo.

7. Kết luận và hạn chế

Mục đích của nghiên cứu này là phân tích tác động của nhận thức an ninh mạng đến nhân viên tại các doanh nghiệp ở Việt Nam. Những kết nối này được nhấn mạnh thông qua việc sử dụng phương pháp nghiên cứu định lượng để phân tích dữ liệu sơ cấp. Việc bảo vệ tài sản thông tin của công ty ngày càng phụ thuộc vào việc nhân viên tuân thủ các quy định bảo mật và hoạt động bảo vệ.

Trong bài báo này, chúng tôi phát triển một mô hình bằng cách kết hợp PMT và TPB để xác định xu hướng tuân thủ hệ thống bảo mật thông tin của nhân viên. Việc nâng cao các khuôn khổ này bằng việc kiểm tra quản trị thể chế cho phép chúng tôi cung cấp sự hiểu biết toàn diện về an ninh mạng. Nghiên cứu này khám phá yếu tố con người trong bảo mật thông tin, cung cấp những cách thức rõ ràng để quản lý và hướng dẫn nhân viên tuân thủ hệ thống bảo mật thông tin. Về cơ bản, nó cung cấp sự hiểu biết có giá trị về bản chất phức tạp của việc bảo vệ tài sản thông tin tại một tổ chức, nêu bật vai trò quan trọng của hành động của nhân viên và sự tương tác giữa các lý thuyết tâm lý và quản trị tổ chức trong việc thiết lập một hệ thống bảo mật thông tin mạnh mẽ.

Mặc dù điều tra này nâng cao hiểu biết của chúng ta về ANM nhưng, điều quan trọng là phải nhận ra một số hạn chế đáng kể. Đầu tiên, mô hình điều tra của chúng tôi không bao gồm tất cả các yếu tố quan trọng, chẳng hạn như kiến thức bảo vệ, rủi ro nhận thức, hỗ trợ đào tạo, can thiệp theo chiều dọc, kinh nghiệm làm việc, văn hóa tổ chức và quản lý hoạt động, những yếu

tố này có thể ảnh hưởng mạnh đến hành vi bảo vệ nhân viên. Vì vậy, các điều tra trong tương lai nên xem xét các nhân tố này khi xây dựng khung điều tra. Thứ hai, điều tra cung cấp bằng chứng mạnh mẽ về tác động trung gian một phần, ngụ ý rằng các yếu tố hoặc con đường khác cũng có thể góp phần vào mối quan hệ. Vì vậy, điều tra trong tương lai nên thực hiện phân tích thực nghiệm để kiểm tra các nhân tố cơ bản ảnh hưởng đến tác động điều tiết của các nhân tố khác. Cuối cùng, điều tra này không phân biệt giữa các loại hình kinh doanh và sở hữu. Do đó, điều tra trong tương lai nên thực hiện phân tích cụm, có thể mang lại kết quả khác nhau.

Chương IV. Làm sáng tỏ các yếu tố ảnh hưởng đến hành vi an ninh mạng của nhân viên: Một cuộc điều tra thực nghiệm trong giới công chức ở Việt Nam

Nội dung chương này được trình bày từ kết quả thăm dò thứ ba đã được công bố:

Tran, D.V., Nguyen, P.V., Vrontis, D., Nguyen, S.T.N. and Dinh, P.U. (2024), "Unraveling influential factors shaping employee cybersecurity behaviors: an empirical investigation of public servants in Vietnam", *Journal of Asia Business Studies*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/JABS-01-2024-0058. Scopus Q1.

Kết quả thăm dò thứ nhất, đã khuyến nghị tới các cơ quan chính phủ và các tổ chức khác nên cung cấp các chương trình đào tạo, hay ban hành chính sách của tổ chức về bảo mật thông tin nhắm mục tiêu cụ thể đến các mối đe dọa bảo mật. Bên cạnh đó, kết quả thăm dò thứ hai, đã nhấn mạnh sự cần thiết của các nhà quản lý ANM cần kết hợp các PP và tài nguyên bảo mật vào văn hóa nơi làm việc để thúc đẩy các EPB an toàn của nhân viên.

Ở thăm dò này chúng tôi tiến hành một cuộc kiểm tra tổng thể tác động của tài khoản GSM và việc tuân thủ PP tổ chức đối với nhận thức, động lực và EPB an ninh mạng của nhân viên chính phủ. Nhân viên phải tuân thủ các chính sách bảo mật thông tin, thực hành bảo mật trực tuyến, sử dụng mạng xã hội, kiểm soát nghiện Internet, đối phó với các mối đe dọa trực tuyến và các thói quen liên quan khác. Kết quả khảo sát từ 330 cán bộ công chức ở Việt Nam được phân tích bằng mô hình phương trình cấu trúc bình phương nhỏ nhất từng phần (PLS-SEM). Kết quả cho thấy, CSA nâng cao động lực và EPB của nhân viên; GSM có tác động tích cực đến CSA và IPM; động cơ bảo vệ thông tin có liên hệ tích cực mạnh mẽ với EPB của nhân viên. Mặc dù tuân thủ PP của tổ chức làm tăng CSA, tác động đến EPB của nhân viên là gián

tiếp. Điều tra này cung cấp cái nhìn sâu sắc về hiệu quả của các sáng kiến ANM của chính phủ và đánh giá toàn diện hơn về nhận thức và EPB bảo vệ thông qua lý thuyết PMT và lý thuyết CT.

1. Giới thiệu

Công nghệ thông tin và truyền thông (ICT) đã được tích hợp sâu sắc trong cơ sở hạ tầng quốc gia và gần như tất cả các khía cạnh của cuộc sống hàng ngày (Li et at., 2022). Sự thâm nhập chưa từng có của CNTT đã giúp các tổ chức đạt được lợi thế cạnh tranh thông qua những cải tiến về khả năng tiếp cận hệ thống, tốc độ và hiệu quả truyền thông cũng như giảm chi phí vận hành (Hasan et at., 2021). Việc áp dụng tài chính kỹ thuật số bị ảnh hưởng nhiều hơn bởi những lợi ích tiềm năng của nó hơn là những rủi ro có thể nhận thấy được (Jain & Raman., 2023). Tuy nhiên, những tiến bộ kỹ thuật số có thể gây ra mối đe dọa an ninh mạng nghiêm trọng cho các tổ chức do tính năng động, tính đa chức năng phức tạp và tính liên kết với nhau của chúng (Fosch-Villaronga & Mahler., 2021; Li et al., 2019). Các cuộc tấn công mạng nhằm vào các doanh nghiệp thuộc mọi quy mô và ngành nghề đang gia tăng về tần suất, số lượng và độ tinh vi (Lu & Xu., 2019). Các cuộc tấn công mạng có thể gây ra thiệt hại nghiêm trọng cho các tổ chức do cố ý hoặc vô ý làm lộ thông tin bí mật (Ou et at., 2022). Tuy nhiên, có những lỗ hổng đáng kể trong hiểu biết của chúng ta về sự khác biệt trong CSA, kiến thức và EPB của nhân viên.

Cách tốt nhất để giảm thiểu hiểm họa tấn công mạng là nâng cao nhận thức của cá nhân. Thuật ngữ "nhận thức về an ninh mạng" đề cập đến mức độ mà các cá nhân hiểu được tầm quan trọng của an ninh thông tin và nghĩa vụ của họ trong việc thực hiện mức độ kiểm soát an ninh thông tin đầy đủ để bảo vệ dữ liệu và mạng của tổ chức (Shaw et at., 2009). Hầu hết các cá nhân không hiểu đầy đủ những công cụ nào cần thiết để bảo vệ khỏi rủi ro mạng (Zwilling et at., 2022). Ngoài ra, khi thế giới ngày càng được kết nối kỹ thuật số, chiến

lược hiệu quả nhất để nâng cao CSA là nâng cao kiến thức của cả người dân và nhân viên trong lĩnh vực kinh doanh và hành chính công (Zwilling et at., 2022). Để làm như vậy, các tổ chức phải thiết lập sự tuân thủ PP. Tuân thủ PP của tổ chức đề cập đến mức độ các cá nhân tuân thủ các quy tắc, quy định, tiêu chuẩn và hướng dẫn được quy định của một tổ chức. Các PP của tổ chức thường bao gồm nhiều lĩnh vực, bao gồm nhưng không giới hạn ở quy tắc ứng xử, bảo mật thông tin, quyền riêng tư dữ liệu, tiêu chuẩn an toàn và thực tiễn nguồn nhân lực. Việc tuân thủ các PP của tổ chức đảm bảo tính đồng nhất, công bằng và hợp pháp trong hoạt động và cách ứng xử của nhân viên hoặc thành viên của tổ chức (AlKalbani et at., 2017; Bauer et at., 2017). Tuy nhiên, các điều tra thực nghiệm về mối quan hệ giữa việc tuân thủ PP với CSA và EPB đã đưa ra những phát hiện trái ngược nhau (Lee et at., 2004; Lee, Y. and Larsen, K.R., 2009); Li et at., 2019). Việc điều tra những mối quan hệ này trong khu vực công của một thị trường mới nổi, chẳng hạn như Việt Nam, có tiềm năng mang lại những hiểu biết mới.

Hơn nữa, vai trò của IPM rất quan trọng trong việc ảnh hưởng đến EPB của nhân viên liên quan đến việc tuân thủ các PP bảo mật thông tin. Cụ thể, IPM là mức độ IPM của nhân viên trong việc thực hiện các biện pháp phòng ngừa chống lại các cuộc tấn công mạng (Ma., 2022; Posey et at., 2015; Vrhovec & Mihelic., 2021). Động lực này là kết quả của quá trình đánh giá mối đe dọa và đối phó và hoạt động như một biến can thiệp tương tự như các động cơ khác nhằm thúc đẩy, duy trì và chỉ đạo các hoạt động của nhân viên (Martens et at., 2019). Theo lý thuyết PMT, nhân viên sẽ thực hiện các biện pháp để tự bảo vệ mình trước các rủi ro an ninh mạng khi họ nhìn thấy mối đe dọa và tin rằng họ có đủ khả năng cần thiết để xử lý mối nguy hiểm tiềm tàng. Tuy nhiên, các cá nhân thường có nhận thức hoặc hiểu biết chưa đầy đủ về cách tự bảo vệ mình trước các cuộc tấn công mạng (Klein & Zwilling., 2023).

Hành vi bảo vệ nhân viên là các bước mà nhân viên thực hiện để giải quyết chính xác các mối lo ngại về an ninh mạng (Li et at., 2019; Tang et at., 2021).

Hệ thống bảo mật thông tin của một tổ chức bị chi phối bởi nhiều nhân tố ở cấp độ cá nhân và tổ chức. Các yếu tố hành vi gần đây đang là tâm điểm chú ý vì nhân viên trực tiếp kiểm soát khả năng tiếp cận, tính bảo mật và tính toàn vẹn của thông tin (Ma., 2022). Hơn 70% vi phạm an ninh là do nhân viên sơ suất hoặc tuân thủ không đầy đủ các giao thức an ninh mạng của tổ chức (Alshaikh et at., 2021). Trong một số trường hợp, nhân viên không nhận thức đầy đủ về nhiều loại tấn công đang liên tục làm thay đổi bối cảnh an ninh của công ty (Zwilling et at., 2022). Ví dụ: việc mở một email có phần mở rộng tệp không quen thuộc hoặc cung cấp quyền truy cập bất hợp pháp cho người khác có khả năng khiến toàn bộ tổ chức gặp phải các vi phạm an ninh mạng. Ngoài ra, nhân viên có xu hướng bỏ qua các biện pháp bảo mật bắt buộc khi hoàn thành nhiệm vụ (Ifinedo., 2012), đặc biệt là khi quản lý nhiều nhiệm vụ cùng lúc và phải đối mặt với thời hạn nghiêm ngặt (Chowdhury et at., 2019). Do đó, với vai trò quan trọng của nhân viên trong ANM, chính phủ và các tổ chức nên kiểm tra và ưu tiên các biện pháp thực hành nhằm nâng cao CSA và EPB của nhân viên một cách hiệu quả.

Phương tiện truyền thông xã hội bao gồm các ứng dụng và nền tảng mạng xã hội là một phần của công nghệ Web 2.0. Những nền tảng này cho phép phát triển, phổ biến và truyền tải kiến thức giữa các cộng đồng người dùng (Del Vecchio et at., 2020). Sự phổ biến ngày càng tăng của những người có ảnh hưởng trên mạng xã hội đã dẫn đến việc áp dụng rộng rãi hoạt động tiếp thị có ảnh hưởng trong chiến lược kinh doanh (Vrontis et at., 2021).

Các tài khoản mạng xã hội (GSM) của chính phủ tăng cường phổ biến thông tin chính thức và cung cấp các nền tảng mới mà công chúng có thể truy cập và mang lại lợi ích (Islm et at., 2021). Cụ thể, GSM là sự hiện diện trực

tuyến được thiết lập và giám sát bởi một cơ quan hoặc tổ chức chính phủ trên nhiều nền tảng truyền thông xã hội khác nhau (Tang et at., 2021). Chính phủ có thể sử dụng GSM để nhanh chóng cung cấp thông tin cho người dân, giúp họ biết về tình trạng của các mối đe dọa, ngăn chặn sự lan truyền dữ liệu sai lệch và hỗ trợ nạn nhân của thảm họa (Guo et at., 2021).

Cụ thể, các nghiên cứu về GSM chủ yếu tập trung vào lý do người dân tương tác với GSM và phân loại các chiến lược nhắn tin khẩn cấp (Tang et at., 2021). Tác động của GSM đối với người dân trong các đợt bùng phát dịch bệnh cấp tính, chẳng hạn như COVID-19 hoặc bệnh sởi, cũng đã được khám phá. Tuy nhiên, có một lỗ hổng đáng chú ý trong việc hiểu tác động của GSM đối với các vấn đề dai dẳng kéo dài hàng thập kỷ, chẳng hạn như các cuộc tấn công an ninh mạng. Sự hiểu biết toàn diện về những tác động này từ góc độ hành vi sẽ giúp các nhà khai thác GSM xây dựng các chiến lược tương tác hiệu quả và tạo ra các thông điệp có giá trị. Tương tự như vậy, các chính phủ có thể sử dụng tài khoản mạng xã hội để nâng cao nhận thức về các mối đe dọa an ninh mạng, nhưng hiệu quả của những nỗ lực này vẫn chưa được xác định. Điều quan trọng là nghiên cứu về việc mở rộng lý thuyết Tuyên truyền trong khuôn khổ GSM còn hạn chế.

Để giải quyết những vấn đề khiếm khuyết trên, điều tra này tích hợp PMT và lý thuyết CT để xem xét tác động của các yếu tố cá nhân (nhận thức và động lực), yếu tố tổ chức (chính sách an ninh mạng) và GSM đối với hành vi bảo vệ của nhân viên liên quan đến ANM. Các câu hỏi điều tra sau đây được đặt ra:

RQ1. Các PP của tổ chức ảnh hưởng như thế nào đến CSA và EPB của nhân viên?

RQ2. GMS ảnh hưởng như thế nào đến CSA và EPB của nhân viên?

RQ3. CSA của nhân viên ảnh hưởng như thế nào đến EPB của họ?

Việc mở rộng khả năng tiếp cận Internet đã làm tăng đáng kể mức độ phức tạp và tần suất của các cuộc tấn công mạng, gây ra những hậu quả bất lợi sâu rộng trong nhiều lĩnh vực, bao gồm các doanh nghiệp, ngành công nghiệp và chính quyền chính trị. Trước những mối nguy hiểm ngày càng tăng này, các chính phủ trên thế giới đã thực hiện các hành động cụ thể để tăng cường an ninh mạng, đặc biệt là những mạng quan trọng đối với quốc phòng. Tại Việt Nam, các cuộc tấn công mạng chủ yếu nhằm vào cơ sở hạ tầng thông tin quan trọng của cơ quan trung ương và các tập đoàn tài chính lớn. Tăng cường cấu trúc pháp lý điều chỉnh an ninh thông tin mạng có thể giúp bảo vệ thông tin quốc phòng quan trọng. Một phần quan trọng của cam kết này là đánh giá năng lực và kiến thức vận hành của những người giám sát mạng, vì việc bảo vệ hiệu quả trước các cuộc tấn công mạng đòi hỏi phải có đội ngũ nhân viên thành thạo. Hơn nữa, việc quản lý an toàn thông tin mạng phù hợp phụ thuộc vào khung pháp lý toàn diện để giảm thiểu rủi ro và giải quyết hiệu quả các mối đe dọa mạng.

Luật An ninh mạng của Việt Nam có hiệu lực từ ngày 01 tháng 01 năm 2019 nêu bật sự nỗ lực của Chính phủ trong việc duy trì trật tự, an toàn xã hội trên không gian mạng. Luật này quy định rõ ràng nhiệm vụ và nghĩa vụ của các cơ quan, công ty và cá nhân có liên quan. Tuy nhiên, cần có các điều tra bổ sung về hướng dẫn và tuân thủ OPC của tổ chức để đảm bảo an toàn và bảo mật cho nhân viên khi họ điều hướng trong lĩnh vực kỹ thuật số, đặc biệt liên quan đến việc sử dụng Internet và giao dịch trực tuyến. Tại Việt Nam, các nền tảng truyền thông xã hội được các tổ chức và quan chức chính phủ sử dụng rộng rãi, trong đó các nền tảng phổ biến dành cho GSM là Facebook, Zalo, Viber, YouTube, TikTok và Instagram.

Điều tra này đóng góp đáng kể vào cơ sở lý luận về ANM ở Việt Nam, đặc biệt là các khía cạnh hành vi, bằng cách đo lường tác động của CSA đối với các EPB thực tế chứ không chỉ đơn thuần là ý định, thái độ và khả năng xảy ra hành vi. Ngoài ra, bằng cách tích hợp bốn thành phần của PMT và lý thuyết Tuyên truyền vào đánh giá CSA, điều tra này cung cấp các thước đo toàn diện về nhận thức về cả các mối đe dọa và các biện pháp đối phó hiện có. Hơn nữa, ảnh hưởng của GSM đến CSA của những người trong tổ chức được điều tra để cung cấp cái nhìn sâu sắc về hiệu quả của những nỗ lực gần đây của chính phủ nhằm thúc đẩy ANM. Cuối cùng, bằng cách xem xét bối cảnh an ninh thông tin của khu vực công, điều tra này cung cấp nền tảng để ban lãnh đạo cấp cao của các tổ chức công đưa ra các quyết định chiến lược về quản trị, sử dụng và vận hành các hệ thống và mạng máy tính.

2. Cơ sở lý thuyết

2.1. Lý thuyết Động cơ bảo vệ

PMT là một khung lý thuyết được thừa nhận rộng rãi để đánh giá các hành vi nhằm giảm thiểu hậu quả bất lợi của các mối đe dọa được nhận thức (Li et at., 2022). Lý thuyết này giải thích rằng sự thay đổi thái độ phụ thuộc vào mức độ động cơ bảo vệ được tạo ra từ quá trình đánh giá nhận thức, bao gồm: PS, PV, RE vàSE (Maddux & Rogers, 1983). PS đề cập đến mức độ, PV và RE của một mối đe dọa rõ ràng như vi-rút máy tính, truy cập trái phép hoặc hack Internet (Hina et at., 2019; Li et at., 2022). PV phản ánh nhận thức của một cá nhân về khả năng xảy ra mối đe dọa hoặc khả năng gặp phải mối đe dọa (Hina et at., 2019; Li et at., 2019; Wong et at., 2022). SE liên quan đến sự đánh giá của một cá nhân về khả năng và kỹ năng cần thiết để thực hiện các hành vi bảo vệ được khuyến nghị nhằm đối phó với các mối đe dọa, chẳng hạn như loại bỏ phần mềm gián điệp khỏi thiết bị điện tử hoặc xử lý các tệp bị nhiễm vi-rút (Hina et at., 2019; Li et at., 2022). SE liên quan đến RE của các

biện pháp đối phó với các cuộc tấn công mạng mà nhân viên có thể thực hiện để ngăn chặn mối đe dọa tiềm tàng (Hina et at., 2019; Li et at., 2019; Wong et at., 2022).

PMT ban đầu được phát triển trong lĩnh vực y tế (Floyd et at., 2000) nhưng sau đó đã được mở rộng sang các lĩnh vực khác, bao gồm bảo mật máy tính và thông tin (Boss et at., 2015). PMT đã được sử dụng để giải thích các hành vi bảo mật thông tin chủ yếu của người dùng nói chung (Van Bavel et at., 2019). Nó cũng được sử dụng để phân tích các hoạt động bảo mật thông tin cá nhân trong nhiều môi trường khác nhau, chẳng hạn như hộ gia đình (Martens et at., 2019), các tổ chức giáo dục đại học (Hina et at., 2019; Hina & Dominic., 2020) và các tổ chức kinh doanh (Li et at., 2019). PMT đặc biệt có lợi trong bối cảnh tổ chức, nơi nhân viên và người dùng cuối cần được khuyến khích thêm để bảo vệ tài sản dữ liệu có giá trị của họ (Li et at., 2022). Ở đây, chúng tôi sử dụng PMT để điều tra các nhân tố quyết định EPB của công chức trong các tổ chức chính phủ, một phân khúc chưa được điều tra kỹ.

2.2. Lý thuyết Tuyên truyền (*Cultivation Theory - CT*)

Lý thuyết Tuyên truyền là một lý thuyết Truyền thông mô tả cách thức đưa tin của các phương tiện truyền thông đại chúng định hình quan điểm của công chúng về các hiện tượng xã hội (Gerbner & Gross., 1976). Lý thuyết Tuyên truyền thừa nhận rằng tần suất sử dụng phương tiện truyền thông cao liên tục sẽ làm tăng sự liên kết của một cá nhân. nhận thức về thực tế xã hội thông qua các mô tả trên phương tiện truyền thông (Tang et at., 2021). Tuyên truyền là một quá trình liên tục và năng động bao gồm hai hình thức: lồng ghép và cộng hưởng (Hermann et at., 2020). Xu hướng chủ đạo đề cập đến sự hội tụ của các quan điểm khác nhau do tiếp xúc với nội dung, trong khi sự cộng hưởng xảy ra khi nội dung truyền thông có mức độ phù hợp cao với trải nghiệm thực tế (Hermann et at., 2020). Phương pháp trau dồi ban đầu tập trung

vào truyền hình nhưng có thể áp dụng cho bất kỳ phương tiện thống trị nào, đặc biệt là mạng xã hội, nhằm củng cố nhận thức và thái độ bằng cách cung cấp một môi trường biểu tượng dễ tiếp cận, hấp dẫn và chia sẻ (Intravia et at., 2017). GSM đã thu hút sự chú ý như một phương tiện tuyên truyền (Tang et at., 2021). So với các cổng web thông thường của chính phủ, mạng xã hội là phương tiện phân phối thông tin hiệu quả hơn và thúc đẩy tương tác hai chiều (Guo et at., 2021).

Cả PMT và lý thuyết Tuyên truyền đều phù hợp cho nghiên cứu này. Nghiên cứu này mở rộng phạm vi của các lý thuyết này để kiểm tra đánh giá của công chức về nhận thức và hành vi bảo vệ an ninh mạng.

2.3. Phát triển giả thuyết

2.3.1. Nhận thức về an ninh mạng, động lực bảo vệ thông tin và hành vi bảo vệ nhân viên

Mặc dù nghiên cứu về nhận thức về an ninh mạng ngày càng tăng nhưng không có một cấu trúc duy nhất nào; các nhà nghiên cứu đã xem xét một số khía cạnh của nhận thức về an ninh mạng (Hanus et at., 2018). Xác định nhận thức về an ninh mạng là điều kiện tiên quyết để nâng cao nhận thức về an ninh mạng (Zwilling et at., 2022). Một số nghiên cứu trước đây đã sử dụng PMT để khái niệm hóa nhận thức về an ninh mạng nhưng chưa xác định rõ ràng cấu trúc này (Lee & Larsen, 2009; Vance et at., 2012). Trong nghiên cứu này, chúng tôi áp dụng quan điểm về mối đe dọa và coi nhận thức về an ninh mạng là một cấu trúc bậc hai bao gồm bốn thành phần: mức độ nghiêm trọng được nhận thức, lỗ hổng được nhận thức, tính tự hiệu quả và hiệu quả phản hồi. Do đó, nhận thức về an ninh mạng là trạng thái mà nhân viên nhận thức được sự xuất hiện và bản chất của các mối đe dọa an ninh mạng, tác động tiềm tàng của các mối đe dọa an ninh mạng đối với an ninh tổ chức (mức độ nghiêm

trọng và lỗ hổng được nhận thức), khả năng của chính họ và các biện pháp dự kiến để ngăn chặn các mối đe dọa đó (năng lực bản thân và hiệu quả đáp ứng).

Theo PMT, mức độ động cơ bảo vệ được khơi gợi phụ thuộc vào việc đánh giá mức độ nghiêm trọng được nhận thức, tính dễ bị tổn thương được nhận thức, tính tự tin vào năng lực bản thân và hiệu quả phản ứng (Maddux & Rogers, 1983). Nếu một mối đe dọa được coi là không nghiêm trọng hoặc không thể xảy ra, nếu không thể thực hiện hành động khả thi nào để giảm thiểu nó hoặc nếu cá nhân nghi ngờ khả năng đối phó với tình huống của mình thì động cơ bảo vệ sẽ không được khơi dậy và ý định hành vi sẽ không thay đổi. Do đó, nhận thức về an ninh mạng cần có ảnh hưởng trực tiếp đến động lực hành động bảo vệ:

H1. CSA có tác động tích cực đến IPM.

Theo PMT, những nhân viên nhận thức rõ hơn về các mối đe dọa trên mạng có nhiều khả năng học cách bảo mật thiết bị của họ hơn, dẫn đến hành vi bảo vệ mạng mạnh mẽ hơn (Klein & Zwilling., 2023). Ví dụ về các hành vi bảo vệ bao gồm thường xuyên thay đổi mật khẩu, tuân thủ các tiêu chuẩn của tổ chức, thận trọng trước khi nhấp vào các liên kết từ các nguồn không xác định, sao lưu dữ liệu, và phần mềm và triển khai các công cụ bảo vệ an ninh mạng (Posey et at., 2015; Tang et at., 2021). Ngược lại, các hành vi rủi ro bao gồm các hoạt động như tiết lộ mật khẩu cá nhân, tải xuống nội dung bất hợp pháp, vi phạm các quy định về bản quyền và bỏ qua các bản cập nhật phần mềm được đề xuất (Zwilling et at., 2022). Nghiên cứu trước đây đã cho thấy tác động trực tiếp của nhận thức về an ninh mạng đối với việc ngăn chặn việc lạm dụng hệ thống thông tin (D'Arcy et at., 2009) và tuân thủ chính sách an ninh mạng (Bulgurcu et at., 2010). Nhận thức về an ninh mạng cao làm tăng đáng kể kiến thức của nhân viên về các mối đe dọa bảo mật và lỗ hổng hệ thống, từ đó nâng cao cảnh giác của họ trước các cuộc tấn công mạng tiềm ẩn,

từ đó đảm bảo rằng thông tin, hệ thống và mạng mà họ tương tác được bảo vệ (Corallo et at., 2022). Mức độ nghiêm trọng được nhận thấy và lỗ hổng được nhận thấy của mối đe dọa tiềm tàng đối với tài sản mạng của tổ chức của họ càng lớn thì khả năng nhân viên sẽ áp dụng các hành vi bảo vệ càng cao và ngược lại (Martens et at., 2019). Tương tự như vậy, nếu một nhân viên tin tưởng mạnh mẽ vào tính hiệu quả của cơ chế đối phó và khả năng thực hiện biện pháp bảo vệ đó, họ sẽ có xu hướng hành động nhiều hơn (Li et at., 2022; Tang et at., 2021). Vì vậy, chúng tôi đề xuất như sau:

H2. CSA có tác động tích cực đến EPB.

2.3.2 Động cơ bảo vệ thông tin và hành vi bảo vệ nhân viên

Một số học giả đã định hình lại động lực bảo vệ thông tin như một thái độ, trong khi những học giả khác bỏ qua động lực bảo vệ thông tin và trực tiếp xem xét giá trị dự đoán của hành vi bảo vệ (có ý định hướng tới) (Wu., 2020). Một số điều tra đã xem xét mối liên hệ giữa động cơ bảo vệ và hành vi thực tế. Mặc dù mục đích chính của PMT là đánh giá IPM nhưng nó có thể được mở rộng để đánh giá các EPB thực tế (Ma., 2022). Vì mục tiêu cuối cùng của điều tra ANM là tăng cường các biện pháp bảo mật thay vì chỉ đơn thuần là ý định nên việc đánh giá các hành vi thực tế là rất có giá trị. Ngoài ra, một phân tích tổng hợp của PMT cho thấy động lực bảo vệ là yếu tố dự báo mạnh mẽ nhất về những thay đổi hành vi (Boss et at., 2015). Do đó, chúng tôi mở rộng PMT bằng cách tích hợp hành vi bảo vệ nhân viên và đưa ra giả thuyết sau:

H3. IPM có tác động tích cực đến EPB của nhân viên.

2.3.3 Truyền thông xã hội của chính phủ và nhận thức về an ninh mạng

Theo lý thuyết CT, việc sử dụng phương tiện truyền thông có thể định hình nhận thức và quan điểm của một cá nhân (Hermann et at., 2020). Sự tham

gia của GSM bao gồm sự tham gia tương tác của những người theo dõi GSM thông qua các hành vi như xem, nhận xét và trao đổi các tin nhắn liên quan đến an ninh mạng bên trong mạng GSM (Tang et at., 2021). Việc tham gia GSM có thể được coi là một hình thức sử dụng phương tiện truyền thông vì nó góp phần nâng cao nhận thức về tình huống của mọi người về một cuộc khủng hoảng mạng (Guo et at., 2021). Những cá nhân tích cực tương tác với các tin nhắn GSM liên quan đến ANM có nhiều khả năng nâng cao CSA mạng hơn (Tang et at., 2021).

Chính xác hơn, việc chính phủ phổ biến thường xuyên các tin tức liên quan đến tội phạm mạng thường xuyên dẫn đến mức độ nhận thức về hiểm họa ngày càng cao trong công chúng. Điều này là do các cá nhân có xu hướng tin rằng các sự kiện được chiếu trên các phương tiện truyền thông có khả năng tác động đến họ hoặc những người thân yêu của họ (Intravia et at., 2017; Shah et at., 2020). Hơn nữa, việc tham gia vào GSM trang bị cho các cá nhân thông tin và hướng dẫn kịp thời để ứng phó hiệu quả với các mối đe dọa tiềm ẩn (Farooq et at., 2020), tạo nền tảng để đánh giá hiệu quả của các phản ứng bảo vệ (Tu et at., 2015). Ngoài ra, sự chuẩn bị nâng cao này sẽ nâng cao niềm tin của các cá nhân vào khả năng tự bảo vệ mình khỏi các mối đe dọa (Tang et at., 2021). Vì vậy, chúng tôi đề xuất như sau:

H4. GSM có tác động tích cực đến CSA.

Để một cá nhân có động lực thực hiện một hành động, họ phải hiểu được mục đích của hành động, nhận ra tầm quan trọng của nó và nhận thức được những kỳ vọng liên quan đến nó (Chen et at., 2018). Sự tham gia của GSM có thể định hình nhận thức và ý kiến của một cá nhân (Guo et at., 2021). Tang (2021) nhận thấy rằng việc tham gia vào GSM góp phần tích cực vào động lực của các cá nhân áp dụng các biện pháp bảo vệ chống lại các hành vi

lừa đảo trên mạng thông qua PS, PV, SE và RE. Dựa trên những lập luận này, đề xuất sau đây;

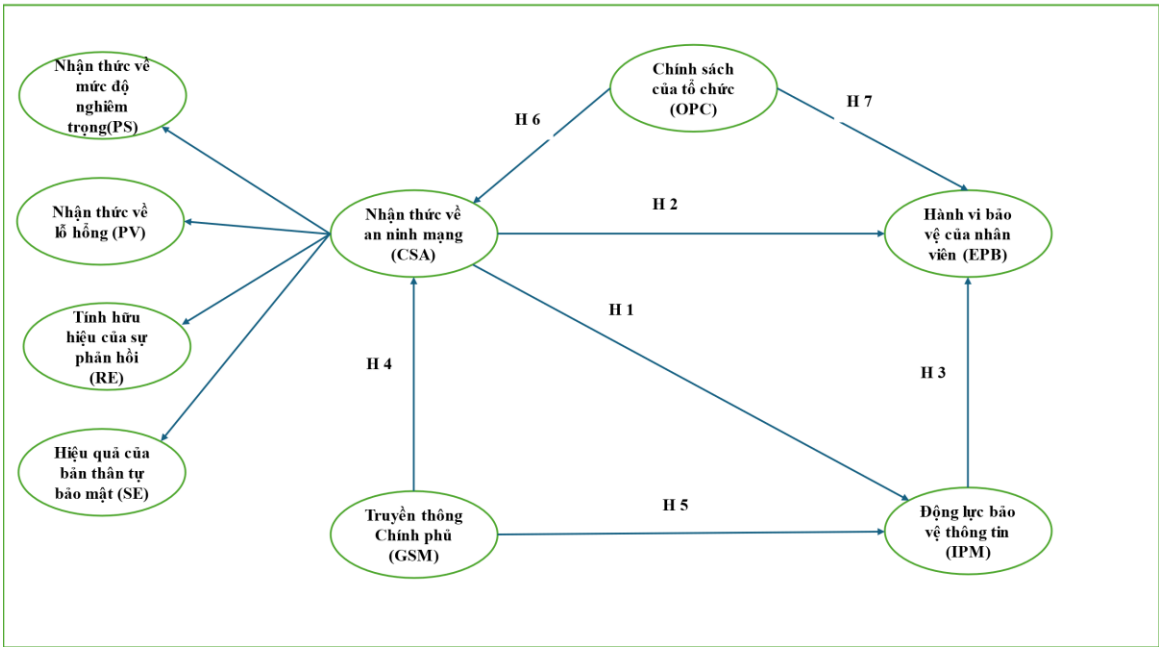
H5. GSM có tác động tích cực đến IPM.

2.3.4. Tuân thủ chính sách của tổ chức, nhận thức về an ninh mạng và hành vi bảo vệ nhân viên

Trên cơ sở khuôn khổ PMT, có thể suy ra rằng những cá nhân có nhận thức cao hơn về các mối đe dọa trên mạng có nhiều khả năng tích cực tìm kiếm thông tin về việc bảo mật thiết bị của họ (Klein & Zwilling., 2023) . Nhận thức được nâng cao này có khả năng làm tăng sự tuân thủ OPC. Việc tuân thủ OPC được nhiều người cho là có ảnh hưởng đáng kể đến EPB của nhân viên và nâng cao mức độ bảo mật thông tin của tổ chức (Chen et at., 2018). OPC an ninh mạng với cơ sở lý luận dễ hiểu có thể ảnh hưởng đến hành vi bảo vệ (D'Arcy et at., 2009; Safa et at., 2015). Tuy nhiên, một số học giả cho rằng nhận thức về OPC an ninh mạng chứ không phải nội dung của OPC ANM ảnh hưởng đáng kể đến ý định lạm dụng máy tính và các hành vi lạm dụng như sửa đổi, đánh cắp hoặc phá hủy phần mềm và dữ liệu (Lee et at., 2004; Lee & Larsen, 2009). Thật vậy, việc nâng cao nhận thức của nhân viên về các chính sách bảo mật góp phần tích cực vào niềm tin của họ về ANM và EPB của họ trong việc bảo vệ an ninh thông tin (Li et at., 2019). Vì các kết quả trước đây trái ngược nhau nên trong điều tra này, chúng tôi điều tra lại mối quan hệ giữa việc tuân thủ OPC và EPB của nhân viên trong bối cảnh cụ thể của các tổ chức chính phủ:

H6. Việc tuân thủ OPC có tác động tích cực đến CSA.

H7. Việc tuân thủ OPC có tác động tích cực đến EPB.



Hình 4.1 tổng hợp các giả thuyết thành mô hình nghiên cứu

Nguồn: Tác giả xây dựng

3. Phương pháp nghiên cứu

3.1. Thang đo

Tất cả các câu hỏi được đánh giá bằng thang đo Likert 7 điểm, từ 1 (rất không đồng ý) đến 7 (rất đồng ý). Các mục đo lường trong bảng câu hỏi được điều chỉnh từ các điều tra trước đó với những sửa đổi nhỏ hoặc lớn. Phần đầu tiên của cuộc khảo sát đã thu thập thông tin nhân khẩu học như giới tính, độ tuổi, trình độ học vấn, thời gian làm việc và quy mô tổ chức. Phần thứ hai bao gồm các câu hỏi và các hạng mục đo lường tương ứng của chúng. Các chỉ số về việc tuân thủ OPC và PS được chỉnh sửa từ Hina et at., (2019). Các câu hỏi về PV và SE được rút ra từ các điều tra trước đây (Hina et at., 2019; Li et at., 2019; Wong et at., 2022). SE được đo lường bằng cách sử dụng các câu hỏi theo Hina et at. (2019) và Li et at. (2022). Các câu hỏi GSM được chỉnh sửa từ Tang et at. (2021). IPM được đánh giá bằng câu hỏi của Ma. (2022) và

Posey et at. (2015). Các câu hỏi về EPB được chỉnh sửa từ Bulgurcu et at. (2010) và Wong et at. (2022).

Bảng 4.1 mô tả cách đo lường tất cả các biến.

Xây dựng (Nguồn)	Số biến	Hạng mục đo lường	Sửa đổi
Chính sách tổ chức (OPC) (Hina et at., 2019)	PP1	Tổ chức của tôi đã thiết lập các quy tắc hành vi cho việc sử dụng máy vi tính theo qui định của tổ chức mình và của Chính phủ.	Sửa đổi lớn
	PP2	Tổ chức của tôi có các hướng dẫn quy tắc sử dụng máy vi tính trong cơ quan tuân thủ theo các quy định của Chính phủ và pháp luật về an ninh mạng.	Sửa đổi lớn
	PP3	Tổ chức của tôi có chính sách cấm nhân viên truy cập vào trang Wesb hay online, khi máy tính của họ chứa các tài liệu quan trọng theo quy định của Chính phủ.	Sửa đổi lớn
	PP4	Tổ chức của tôi đã xác lập bộ quy tắc ứng xử, giải thích những điều nên làm và không nên làm trong bảo mật an ninh thông tin theo quy định của Nhà nước.	Sửa đổi lớn
Nhận thức về ANM PMT: Nhận thức về an ninh mạng (CSA) (Bulgurcu et al., 2010)	GCA1	Nhìn chung, tôi nhận thức được các mối đe dọa về bảo mật *(an ninh mạng)* an toàn thông tin và hậu quả tiêu cực của chúng.	Sửa đổi lớn
	GCA2	Tôi có đủ kiến thức nhận biết về hậu quả của việc thông tin (*an ninh mạng*) bị mất cắp.	Sửa đổi lớn
	GCA3	Tôi hiểu những lo ngại về an ninh mạng liên quan đến bảo mật thông tin và những rủi ro khi thông tin bị mất cắp.	Sửa đổi lớn
Nhận thức về ANM PMT: Mức độ nghiêm trọng được cảm nhận (Hina et al., 2019)	PS1	Việc bảo vệ thông tin *(an ninh mạng)* của tổ chức tôi rất quan trọng.	Sửa đổi lớn
	PS2	Tại nơi làm việc, việc truy cập thông tin riêng tư của tôi mà không có sự đồng ý của tôi đó là một vấn đề nghiêm trọng đối với tôi.	Sửa đổi lớn
	PS3	Tôi hiểu rằng việc có ai đó xâm phạm thành công hoặc làm hỏng tài nguyên thông tin của tôi tại nơi làm việc là rất nguy hiểm.	Sửa đổi lớn

	PS4	Mất dữ liệu do hacker là một vấn đề nghiêm trọng đối với tôi.	Sửa đổi lớn
	PS5	Việc tổ chức đào tạo nhân viên sẽ là bước quan trọng đảm bảo việc bảo mật an toàn thông tin *(an ninh mạng)*.	Sửa đổi lớn
	PS6	Có thể giảm bớt rủi ro khi nhân viên nhận thức rõ hơn về các mối đe dọa an ninh mạng và hậu quả của nó, xuất phát từ sự sơ suất của họ.	Sửa đổi lớn
	PS7	Thông qua giáo dục, cung cấp kiến thức và thông tin đầy đủ giúp nâng cao nhận thức của nhân viên về bảo mật an toàn thông tin *(an ninh mạng)*.	Sửa đổi lớn
Nhận thức về ANM PMT: Nhận thức được lỗ hổng (Hina. et al., 2019); Li et at., 2019; Wong et at., 2022)	PV1	Tôi biết rằng tổ chức của tôi có thể dễ xuất hiện vi phạm bảo mật *(an ninh mạng),* nếu tôi không tuân thủ Chính sách Bảo mật Thông tin *(an ninh mạng)* của tổ chức tôi.	Sửa đổi lớn
	PV2	Tôi có thể trở thành nạn nhân của một cuộc tấn công có mục đích nếu tôi không tuân thủ Chính sách Bảo mật an toàn thông tin *(an ninh mạng)* của tổ chức tôi.	Sửa đổi lớn
	PV3	Về rủi ro bảo mật an toàn thông tin tại nơi làm việc của tôi, tài nguyên *(dữ liệu)* máy tính của tôi có thể dễ bị tấn công.	Sửa đổi lớn
	PV4	Tôi tin rằng mỗi cá nhân có ý thức và nỗ lực bảo vệ an toàn thông tin *(an ninh mạng)* của tổ chức, sẽ làm giảm nguy cơ truy cập bất hợp pháp và mất an toàn thông tin.	Sửa đổi lớn
	PV5	Các tổ chức nên đầu tư sử dụng các công nghệ bảo vệ an ninh mạng hiện đại.	Sửa đổi lớn
	PV6	Tổ chức cần thường xuyên thông báo cho nhân viên về các mối đe dọa an ninh mạng tiềm ẩn.	Sửa đổi lớn
	PV7	Nhiều nguy cơ tiềm ẩn về vi phạm bảo mật an toàn thông tin *(an ninh mạng)* sẽ xảy ra đối với hệ thống máy tính của tổ chức tôi.	Sửa đổi lớn
Nhận thức về ANM PMT: Hiệu quả của bản thân tự bảo mật	SE1	Tôi tin rằng tôi có các kỹ năng cần thiết để tự bảo vệ mình khỏi các hành vi vi phạm an toàn thông tin *(an ninh mạng)*.	Sửa đổi lớn
	SE2	Tôi tin rằng tôi đã phát triển khả năng ngăn chặn mọi người lấy cắp thông tin bí mật của tôi.	Sửa đổi lớn

(Hina et at., 2019; Li et at., 2022)	SE3	Tôi bật các biện pháp bảo mật *(tường lửa, chống vi-rút, v.v.)* trên tài nguyên máy tính công việc của mình.	Sửa đổi lớn
	SE4	Tôi tin rằng việc tự bảo vệ mình khỏi các hành vi vi phạm bảo mật an toàn thông tin *(an ninh mạng)*, nằm trong tầm kiểm soát của tôi.	Sửa đổi lớn
	SE5	Tôi tự tin khi mở duyệt trình web ở các mức độ bảo mật khác nhau.	Sửa đổi lớn
	SE6	Tôi cảm thấy tự tin khi xử lý các file bị nhiễm virus.	Sửa đổi lớn
	SE7	Tôi cảm thấy tự tin khi loại bỏ các phần mềm gián điệp và phần mềm độc hại khỏi máy tính.	Sửa đổi lớn
Nhận thức về ANM PMT: Hiệu quả đáp ứng (Hina et at., 2019; Li et at., 2019; Wong et at., 2022)	RE1	Trong tổ chức của tôi, những nỗ lực để đảm bảo an toàn thông tin *(an ninh mạng)*, bí mật của tôi là có hiệu quả.	Sửa đổi lớn
	RE2	Tại tổ chức của tôi, các biện pháp bảo mật *(an ninh mạng)* hiện có để bảo vệ an toàn thông tin, công việc của tôi khỏi các vi phạm bảo mật *(an ninh mạng)* đều có hiệu lực.	Sửa đổi lớn
	RE3	Các biện pháp phòng ngừa an ninh mạng có sẵn cho tôi tại tổ chức của tôi, để đối phó với nội dung độc hại, đều có hiệu quả.	Sửa đổi lớn
	RE4	Các biện pháp bảo mật an toàn thông tin *(an ninh mạng)* tại tổ chức của tôi đã ngăn chặn tin tặc truy cập vào thông tin cá nhân hoặc giáo dục nhạy cảm.	Sửa đổi lớn
	RE5	Việc tuân thủ các chính sách bảo mật an toàn thông tin trong tổ chức sẽ ngăn chặn các vi phạm bảo mật an toàn thông tin, an ninh mạng.	Sửa đổi lớn
	RE6	Nếu tôi tuân thủ các chính sách bảo mật thông tin *(an ninh mạng)*, khả năng xảy ra vi phạm an toàn thông tin *(an ninh mạng)* sẽ giảm xuống.	Sửa đổi lớn
	RE7	Tuân thủ cẩn thận các chính sách bảo mật thông tin giúp tránh các vấn đề về an ninh mạng.	Sửa đổi lớn
	RE8	Tổ chức có thể cải thiện an toàn thông tin *(an ninh mạng)* khi người dùng chỉ ra được sơ suất về bảo mật *(an ninh mạng)* của họ đến tình hình an ninh mạng của tổ chức.	Sửa đổi lớn

	RE9	Tổ chức nên có Quy định chung về Bảo vệ Dữ liệu *(an ninh mạng).*	Sửa đổi lớn
	RE10	Tổ chức nên thường xuyên nâng cấp phần mềm chống vi-rút và tường lửa.	Sửa đổi lớn
Truyền thông của chính phủ (Tang et at., 2021)	GSM1	Tôi luôn đọc và nghe các khuyến cáo về an ninh mạng được Chính phủ đăng tải.	Sửa đổi lớn
	GSM2	Tôi luôn chia sẻ các khuyến cáo về an ninh mạng được Chính phủ đăng tải.	Sửa đổi lớn
	GSM3	Tôi luôn truyền đạt các khuyến cáo về an ninh mạng được Chính phủ đăng tải.	Sửa đổi lớn
Động lực bảo vệ thông tin (Ma., 2022; Posey et at., 2015)	IPM1	Tôi dự định bảo vệ tổ chức của mình khỏi các mối đe dọa về an toàn thông tin *(an ninh mạng)*.	Sửa đổi lớn
	IPM2	Mức độ thành công trong việc ngăn chặn các mối đe dọa về an ninh mạng, bảo mật thông tin của tổ chức là rất cao.	Sửa đổi lớn
	IPM3	Tôi luôn sẵn sàng tham gia vào các hoạt động bảo vệ hệ thống thông tin khỏi các mối đe dọa an ninh mạng.	Sửa đổi lớn
	IPM4	Tôi luôn nỗ lực bảo vệ tổ chức của mình khỏi các mối đe dọa về bảo mật thông tin *(an ninh mạng)*.	Sửa đổi lớn
	IPM5	Tôi sẽ cố gắng hết sức để ngăn chặn các mối đe dọa về bảo mật thông tin *(an ninh mạng)* xảy ra trong tổ chức của mình.	Sửa đổi lớn
Hành vi bảo vệ của nhân viên (Li et at., 2019)	EPB1	Tôi luôn cập nhật phần mềm chống vi-rút trên máy tính của mình.	Sửa đổi lớn
	EPB2	Tôi theo dõi các dấu hiệu bất thường của máy tính (ví dụ: máy tính chạy chậm hoặc bị treo, nhiều cửa sổ bật lên, v.v.).	Sửa đổi lớn
	EPB3	Tôi luôn quan tâm bất kỳ phần mềm độc hại nào được cảnh báo qua các kênh thông tin truyền thông.	Sửa đổi lớn

3.2. Thu thập dữ liệu

Cuộc khảo sát ban đầu được viết bằng tiếng Anh và sau đó được dịch sang tiếng Việt để tạo điều kiện phổ biến tới nhiều đối tượng tham gia hơn. Một nghiên cứu thí điểm trên 30 người trả lời đã được thực hiện để đánh giá

tính phù hợp của bản dịch trong bối cảnh tiếng Việt. Dựa trên kết quả, các sửa đổi đã được thực hiện để cải thiện tính rõ ràng và dễ đọc của bảng câu hỏi. Từ tháng 10 năm 2022 đến tháng 3 năm 2023, dữ liệu được thu thập bằng cách phân phát khảo sát cho các công chức đang làm việc tại các tổ chức chính phủ. Chúng tôi đã nhận được sự hỗ trợ quý giá từ chính quyền địa phương trong việc phân phối bản khảo sát đến các tổ chức của họ.

Dữ liệu được thu thập bằng cách áp dụng các phương pháp phi xác suất, cụ thể là phương pháp phân tầng. Theo cách tiếp cận này, bảng câu hỏi được gửi tới 200 cán bộ công chức tại mỗi khu vực của Thành phố Hồ Chí Minh và Thủ đô Hà Nội. Ngoài ra, 150 khảo sát đã được phổ biến tại 2 tỉnh lân cận là tỉnh Đồng Nai và tỉnh Bình Dương. Tổng cộng, 700 bảng câu hỏi đã được phân phát và 564 bảng câu hỏi được trả về, trong đó có 330 câu trả lời hợp lệ.

3.3. Phương pháp nghiên cứu

Mô hình phương trình cấu trúc bình phương nhỏ nhất từng phần (PLS-SEM) được sử dụng để phân tích dữ liệu và đánh giá mô hình điều tra. PLS-SEM là một phương pháp tiếp cận dựa trên phương sai nhằm đánh giá các cấu trúc mô hình từng phần bằng cách tích hợp phân tích thành phần chính và hồi quy bình phương nhỏ nhất thông thường (Hair et at., 2020). PLS-SEM được sử dụng rộng rãi trong một số lĩnh vực, bao gồm cả nghiên cứu về hành vi an ninh mạng (Alanazi et at., 2022; Wong et at., 2022). PLS-SEM phù hợp tốt với mục tiêu nghiên cứu của chúng tôi vì nhiều lý do. Đầu tiên, nó có thể kiểm tra khung lý thuyết từ quan điểm dự đoán. Thứ hai, nó cung cấp hỗ trợ cho mô hình cấu trúc, mô hình phức tạp và bao gồm nhiều cấu trúc, chỉ báo, thành phần phụ thuộc và mối quan hệ mô hình. Cuối cùng, nó nâng cao khả năng hiểu khi khám phá phần mở rộng của các lý thuyết đã được thiết lập (Hair et at., 2019).

4. Kết quả

4.1. Đặc điểm dân số

Hồ sơ nhân khẩu học và đặc điểm tổ chức của người trả lời được thể hiện trong Bảng 4.2. Trong số những người trả lời, 26,67% là nam giới và 74,0% là nữ. Phần lớn (71,21%) là độ tuổi 18-35. Hơn 72% người tham gia có bằng cử nhân trở lên, 66,97% có trên 5 năm kinh nghiệm làm việc và 52,42% làm việc tại các tổ chức lớn có hơn 100 nhân viên.

Bảng 4.2. Đặc điểm nhân khẩu học

Mục nhân khẩu học		Số mẫu (N = 330	Tỷ lệ (%)
Giới tính	Nữ	88	26.67%
	Nam	242	73.33%
Tuổi tác	18 tới 35 tuổi	235	71.21%
	36 tới 45 tuổi	73	22.12%
	Trên 45 tuổi	22	6.67%
Trình độ học vấn	Trung học phổ thông	90	27.27%
	Đại học	185	56.06%
	Sau đại học	55	16.67%
Kinh nghiệm làm việc	Ít hơn 3 năm	49	14.85%
	Từ 3 năm tới 5 năm	60	18.18%
	Nhiều hơn 5 năm	221	66.97%
Quy mô tổ chức	Ít hơn 50 nhân viên	98	29.70%
	51 tới 100 nhân viên	59	17.88%
	Nhiều hơn 100 nhân viên	173	52.42%

Nguồn: Được tạo bởi các tác giả.

4.2. Xu hướng phương pháp phổ biến

Phương pháp được sử dụng trong nghiên cứu này làm tăng nguy cơ sai lệch phương pháp chung (CMB) vì hướng dẫn câu hỏi và mức độ mong muốn của xã hội có thể ảnh hưởng đến câu trả lời của người trả lời, dẫn đến sự khác biệt chung giữa các chỉ số (Kock., 2015). Các yếu tố lạm phát phương sai cộng tuyến đầy đủ (FCVIF) có thể phát hiện CMB một cách hiệu quả, ngay cả trong một mô hình đáp ứng các tiêu chí tiêu chuẩn về giá trị hội tụ và phân biệt dựa trên phân tích nhân tố xác nhận (Kock., 2015). Nếu tất cả FCVIF thu được thông qua kiểm tra cộng tuyến đầy đủ đều bằng 3,3 hoặc nhỏ hơn thì mô hình được coi là không có CMB (Kock., 2015). Như được hiển thị trong Bảng 4.3, FCVIF cho tất cả các cấu trúc tiềm ẩn đều dưới ngưỡng 3,3, ngụ ý rằng dữ liệu được thu thập không bị ảnh hưởng bởi CMB.

4.3 Hiệu lực và độ tin cậy

Số liệu thống kê kiểm tra độ tin cậy và giá trị của các biện pháp xây dựng được trình bày trong Bảng 4.3 và Bảng 4.4. Nên tải hệ số vượt quá 0,70 để đảm bảo độ tin cậy của hạng mục có thể chấp nhận được (Hair et at., 2020) . Như được hiển thị trong Bảng 4.4, tất cả các chỉ báo đều thể hiện hệ số tải vượt quá ngưỡng này ngoại trừ RE10 có hệ số tải là 0,662. Do đó, RE10 đã bị loại khỏi phân tích.

Độ tin cậy nhất quán nội bộ có thể được đánh giá bằng cách sử dụng cả độ tin cậy Cronbach's alpha (a) và độ tin cậy tổng hợp (CR); các giá trị lớn hơn 0,70 được khuyến nghị cho cả hai thước đo độ tin cậy (Hair et at., 2020). Bảng 4.4 cho thấy tất cả các cấu trúc đều có cả giá trị a và CR trên 0,70, cho thấy độ tin cậy đạt yêu cầu đến tốt.

Giá trị trích xuất phương sai trung bình (AVE) từ 0,50 trở lên biểu thị rằng cấu trúc chiếm ít nhất 50% phương sai trong các mục của nó (Hair et at.,

2020). Trong nghiên cứu này, tất cả các giá trị AVE của các cấu trúc đều cao hơn 0,50, ngụ ý rằng kiểm tra tính giá trị hội tụ được thỏa mãn.

Bảng 4.3. Phân tích nhân tố với số liệu thống kê về độ tin cậy và giá trị

Tên biến	Ký hiệu	Hệ số tải tải (>0.7)	Alpha (>0.7)	CR (> 0.7)	AVE(>0.5)	FCVIF (<3.3)
Hành vi bảo vệ của nhân viên (EPB)	EPB1 EPB2 EPB3	0.918 0.936 0.920	0.915	0.917	0.855	2.880
Truyền thông chính phủ (GSM)	GSM1 GSM2 GSM3	0.911 0.919 0.905	0.899	0.899	0.831	3.255
Động lực bảo vệ thông tin (IPM)	IPM1 IPM2 IPM3 IPM4 IPM5	0.895 0.892 0.903 0.932 0.920	0.947	0.947	0.825	1.106
Chính sách của tổ chức (OPC)	OPC1 OPC2 OPC3 OPC4	0.893 0.933 0.872 0.919	0.926	0.927	0.818	2.182
Nhận thức về ANM (biến bậc hai)						

Nhận thức về mức độ nghiêm trọng (PS)	PS1 PS2 PS3 PS4 PS5 PS6 PS7	0.845 0.818 0.802 0.847 0.811 0.825 0.850	0.924	0.926	0.686	1.838
Nhận thức về lỗ hổng (PV)	PV1 PV2 PV3 PV4 PV5 PV6 PV7	0.796 0.792 0.815 0.776 0.785 0.782 0.814	0.903	0.906	0.631	1.484
Tính hữu hiệu của sự phản hồi (RE)	RE1 RE2 RE3 RE4 RE5 RE6 RE7 RE8 RE9 RE10	0.873 0.865 0.841 0.828 0.795 0.805 0.801 0.841 0.705 Loại	0.938	0.942	0.670	2.516

Hiệu quả của bản thân tự Bảo mật (SE)	SE1	0.847	0.943	0.944	0.745	2.475
	SE2	0.898				
	SE3	0.824				
	SE4	0.895				
	SE5	0.908				
	SE6	0.827				
	SE7	0.836				

Nguồn: Được tạo bởi các tác giả.

Cuối cùng, giá trị phân biệt được kiểm tra bằng cách sử dụng tỷ lệ dị tính-đơn tính trạng (HTMT) và tiêu chí Fornell- Larcker (Hair et at., 2020). Tỷ lệ HTMT so sánh mối tương quan của một mục giữa các cấu trúc với mối tương quan của nó với cùng một cấu trúc và ranh giới trên là 0,85 hoặc 0,90 (Hair et at., 2019) được đề xuất để tránh các vấn đề về giá trị phân biệt đối xử. Tiêu chí Fornell-Larcker được đáp ứng khi bình phương AVE của một yếu tố vượt quá căn bậc hai của các mối tương quan giữa các cấu trúc của nó (Fornell, C. and Larcker, D.F., 1981). Như được hiển thị trong Bảng 4.4, tất cả các cấu trúc đều đáp ứng các yêu cầu cho cả tỷ lệ HTMT và tiêu chí Fornell-Larcker, ngụ ý mức độ giá trị phân biệt có thể chấp nhận được.

Bảng 4.4. Tỷ lệ HTMT và tiêu chí Fornell-Larcker

Tên biến	EPB	OPC	GMS	IPM	PS	PV	RE	SE
Tỷ lệ HTMT								
Hành vi bảo vệ của nhân viên (EPB)								
Chính sách của tổ chức (OPC)	0.745							

Truyền thông của Chính phủ (GSM)	0.855	0.849						
Động lực bảo vệ thông tin (IPM)	0.864	0.761	0.799					
Nhận thức về mức độ nghiêm trọng (PS)	0.667	0.594	0.601	0.728				
Nhận thức về lỗ hổng (PV)	0.457	0.417	0.394	0.473	0.592			
Tính hữu hiệu của sự phản hồi (RE)	0.743	0.820	0.760	0.827	0.747	0.514		
Hiệu quả của bản thân tự bảo mật (SE)	0.724	0.684	0.719	0.688	0.531	0.488	0.813	
Tiêu chí Fornell-Larcker								
Hành vi bảo vệ của nhân viên (EPB)	**0.925**							
Chính sách của tổ chức (OPC)	0.685	**0.904**						
Truyền thông của chính phủ (GSM)	0.775	0.773	**0.912**					
Động lực bảo vệ thông tin (IPM)	0.805	0.713	0.737	**0.908**				
Nhận thức về mức độ nghiêm trọng (PS)	0.615	0.550	0.549	0.682	**0.828**			
Nhận thức về lỗ hổng (PV)	0.420	0.387	0.359	0.440	0.540	**0.794**		
Tính hữu hiệu của sự phản hồi (RE)	0.695	0.766	0.703	0.782	0.691	0.472	**0.818**	
Hiệu quả của bản thân tự bảo mật (SE)	0.671	0.640	0.663	0.650	.0501	0.457	0.775	**0.863**

Lưu ý: Căn bậc hai của AVE được in đậm trên các đường chéo

Nguồn: Được tạo bởi các tác giả.

4.4. Đánh giá mô hình kết cấu

Vì không có số liệu thống kê về mức độ phù hợp tiêu chuẩn cho PLS-SEM nên chất lượng của mô hình được đánh giá dựa trên khả năng dự đoán các cấu trúc nội sinh của nó (Hair et at., 2019). Việc đánh giá này được hướng dẫn bởi hệ số xác định (R^2) và quy mô hiệu ứng (f^2) (Hair et at., 2019).

R^2 biểu thị tác động chung của các biến ngoại sinh lên các biến nội sinh và nằm trong khoảng từ 0 đến 1, với 1 biểu thị độ chính xác dự đoán tuyệt đối (Hair et at., 2019). Các giá trị R^2 lần lượt là 0,75, 0,50 và 0,25 được hiểu là biểu thị độ chính xác dự đoán đáng kể, trung bình và yếu (Hair et at., 2019). Trong mô hình của chúng tôi, giá trị R^2 của ba biến nội sinh—CSA, IPM và EPB—lần lượt là 0,614, 0,654 và 0,682. Những giá trị này cho thấy độ chính xác dự đoán từ trung bình đến đáng kể.

f^2 được sử dụng để đánh giá tác động của việc loại bỏ cấu trúc yếu tố dự đoán cụ thể đối với R^2 của một biến nội sinh (Hair et al., 2019). f^2 các giá trị 0,02, 0,15 và 0,35 lần lượt biểu thị kích thước hiệu ứng nhỏ, trung bình và lớn. Các mối quan hệ được điều tra trong điều tra này có mức độ ảnh hưởng trung bình hoặc lớn, ngoại trừ mối quan hệ giữa CSA và EPB cũng như giữa việc tuân thủ OPC và EPB, có giá trị f^2 lần lượt là 0,031 và 0,028.

4.5 Kiểm định giả thuyết

Kết quả kiểm định giả thuyết được trình bày ở Bảng 4.5 Giả thuyết được chấp nhận khi giá trị p < 0,05 hoặc giá trị t tương ứng >1,96; nếu không, nó bị từ chối. Tất cả các giả thuyết đều được ủng hộ ngoại trừ H7. CSA ảnh hưởng tích cực đến IPM và EPB (P = 0,501, p = 0,175, p < 0,05), ủng hộ H1 và H2. GSM ảnh hưởng tích cực đến CSA và IPM(P = 0,375, p = 0,365, p < 0,05); do đó, H3 và H4 được chấp nhận. Mối tương quan giữa IPM và EPB là tích cực đáng kể (P = 0,562, p = 0,000), ủng hộ H5. Việc tuân thủ OPC nâng cao mạnh mẽ CSA(P = 448, p < 0,05), khẳng định H6. Tuy nhiên, H7, cho thấy

tác động tích cực của việc tuân thủ OPC đối với EPB, bị từ chối vì giá trị p là 0,109 và giá trị t là 1,604 của nó không đáp ứng các ngưỡng được khuyến nghị.

Bảng 4.5. Kết quả kiểm định giả thuyết

	Giả thuyết	β	t-value	p-value	Nhận xét
H1	CSA → EPB	0.188	2.335	0.020	Chấp nhận
H2	CSA → IPM	0.493	7.161	0.000	Chấp nhận
H3	GSM → CSA	0.359	4.102	0.000	Chấp nhận
H4	GSM → IPM	0.379	4.918	0.000	Chấp nhận
H5	IPM → EPB	0.555	6.025	0.000	Chấp nhận
H6	OPC → CSA	0.476	6.023	0.000	Chấp nhận
H7	OPC → EPB	0.148	1.592	0.111	Không Chấp nhận

Ghi chú: CSA: Nhận thức về an ninh mạng; EPB: Hành vi bảo vệ nhân viên; IPM: Động lực bảo vệ thông tin; GSM: Truyền thông xã hội của chính phủ; OPC: Tuân thủ chính sách tổ chức.

4.6. Hiệu ứng trung gian

Tác động gián tiếp được đánh giá để đánh giá ba mối quan hệ trung gian tiềm năng: (1) IPM với tư cách là trung gian hòa giải mối quan hệ giữa CSA và EPB; (2) CSA như một trung gian hòa giải mối quan hệ giữa GSM và IPM; và (3) CSA với vai trò là trung gian hòa giải mối quan hệ giữa việc tuân thủ OPC và EPB. Như được hiển thị trong Bảng 4.6, tác động trực tiếp và gián tiếp trong hai mối quan hệ đầu tiên là tích cực đáng kể (P > 0 và p <0,05). Đối

với mối quan hệ thứ ba, tác động trực tiếp không được hỗ trợ, nhưng tác động gián tiếp lại tích cực đáng kể (P = 0,079 và p = 0,05). Đối với hai mối quan hệ đầu tiên, tác động gián tiếp và trực tiếp có cùng hướng, biểu thị sự điều hòa bổ sung. Ngược lại, CSA làm trung gian hoàn toàn cho mối quan hệ giữa việc tuân thủ OPC và EPB.

Bảng 4.6. Hiệu ứng trung gian

Giả thuyết		Loại	β	Giá trị - t	Giá trị - p	Nhận xét
H1.	CSA → EPB CSA → IPM → EPB	Trực tiếp Gián tiếp	0.188 0.274	2.335 4.947	0.020 0.000	Chấp nhận Bổ sung (một phần)
H4.	GSM → IPM GSM → CSA → IPM	Trực tiếp Gián tiếp	0.379 0.177	4.918 3.487	0.000 0.000	Chấp nhận Bổ sung (một phần)
H7.	OPC → EPB OPC → CSA → EPB	Trực tiếp Gián tiếp	0.148 0.068	1.592 1.806	0.111 0.071	Không Chấp nhận Chỉ gián tiếp

Nguồn: Được tạo bởi các tác giả.

4.7. Cuộc thảo luận

Điều tra này xem xét việc tuân thủ OPC và GSM ảnh hưởng như thế nào đến CSA, IPM và EPB của nhân viên. Những phát hiện của chúng tôi chứng minh sáu trong số bảy giả thuyết được đề xuất. Cụ thể, CSA được cho là có tác động tích cực đến IPM và ảnh hưởng tích cực trực tiếp đến EPB, phù hợp với một điều tra trước đây (Tang et at., 2021; Wong et at., 2022) cũng quan sát thấy rằng CSA cải thiện đáng kể trình độ của nhân viên trong việc xử lý các nhiệm vụ an ninh mạng nhằm ứng phó với các mối đe dọa được nhận thấy và nhận thức đã được chứng minh là có tác động trực tiếp đến việc ngăn

chặn hành vi lạm dụng trên mạng và việc tuân thủ OPC (Bulgurcu et at., 2010; D'Arcy et at., 2009). Ngoài ra, người ta thấy có mối tương quan tích cực đáng kể giữa IPM và EPB. Kết quả này phù hợp với nghiên cứu của Ma. (2022), người đã kết luận rằng IPM là một yếu tố dự báo mạnh mẽ về hành vi. IPM cũng phần nào làm trung gian cho mối quan hệ giữa CSA và EPB.

GSM có ảnh hưởng tích cực đến CSA nhất quán với các đề xuất trước đây rằng GSM là nguồn thông tin chính liên quan đến khủng hoảng (Intravia et at., 2017; Shah et at., 2020; Tang et, al., 2021). Sự tham gia tích cực với GSM không chỉ khiến các cá, nhân tin rằng các sự kiện truyền thông liên quan đến tấn công mạng có thể ảnh hưởng đến họ mà còn trang bị cho họ kiến thức và sự chuẩn bị cần thiết để ứng phó hiệu quả, từ đó nâng cao CSA. CSA cũng phần nào làm trung gian cho mối quan hệ giữa GSM và IPM. Quan sát này phù hợp với những phát hiện của Tang et at. (2021), người cho rằng việc sử dụng thông tin trên mạng xã hội sẽ thúc đẩy người dùng thực hiện các hành động phòng ngừa. Bằng cách chứng minh tác động trực tiếp của GSM đến IPM, điều tra này cung cấp một góc nhìn mới, vì điều tra trước đây chủ yếu điều tra ảnh hưởng của GSM đến IPM và EPBi bằng cách đo lường các biến số như nỗi sợ bị coi là nạn nhân.

Cuối cùng nhưng không kém phần quan trọng, việc tuân thủ OPC sẽ nâng cao đáng kể CSA. Tuy nhiên, việc tuân thủ OPC không có tác động trực tiếp đến EPB; thay vào đó, mối quan hệ này hoàn toàn được điều chỉnh bởi CSA. Hina et at. (2019) đề xuất rằng để tăng cường hành vi và hành động bảo mật, các tổ chức phải vượt ra ngoài việc phân phối các chính sách an ninh mạng của tổ chức và đảm bảo sự quen thuộc với nội dung của chúng; nhân viên phải nhận thức đầy đủ PS của vi phạm an ninh và khả năng PV của tổ chức đối với vi phạm đó. Vai trò trung gian của CSA nhấn mạnh tầm quan trọng của việc không chỉ xây dựng OPC an ninh mạng mà còn thực hiện các

quy trình để phổ biến và thấm nhuần chính sách đó vào tâm trí nhân viên nhằm nâng cao EPB.

5. Ý nghĩa và kết luận

5.1. Đóng góp lý thuyết

Đầu tiên, điều tra hiện tại cung cấp một phân tích toàn diện về tài liệu về nhận thức, động lực và hành vi về an ninh mạng. Điều tra này mở rộng PMT và lý thuyết CT bằng cách kết hợp EPB như một yếu tố quan trọng và kiểm tra mối liên hệ giữa khái niệm này và IPM. Đánh giá các hành động thực tế là một thành phần thiết yếu của điều tra an ninh mạng, vì mục tiêu chính là tăng cường các biện pháp bảo mật chứ không chỉ là ý định. Nghiên cứu này chứng minh rằng CSA và IPM đều ảnh hưởng đáng kể đến EPB.

Thứ hai, điều tra này tích hợp bốn nhân tố CSA (mức độ nghiêm trọng được nhận thức, tính dễ bị tổn thương được nhận thức, tính tự -hiệu quả và hiệu quả phản hồi) để tạo ra cấu trúc bậc hai về CSA. Cấu trúc đa chiều này phản ánh sự phức tạp của nhận thức về an ninh mạng đồng thời đơn giản hóa mô hình và giảm số lượng giả thuyết, cho phép chúng ta tập trung vào những gì thực sự quan trọng và khám phá những hiểu biết sâu sắc có ý nghĩa.

Thứ ba, khung khái niệm của chúng tôi kết hợp các tác động của việc trau dồi thông qua GSM để điều tra các tiền đề của CSA. Tài liệu chủ yếu tập trung vào việc tìm hiểu lý do tại sao các cá nhân sử dụng GSM trong các cuộc khủng hoảng và phân loại các chiến lược nhắn tin khẩn cấp được GSM sử dụng (Tang et at., 2021). Những điều tra này bỏ qua tác động của GSM đối với CSA và IPM của cá nhân đối với các vấn đề cấp bách lâu năm như OPC, đặc biệt khi các cá nhân nhiệt tình tham gia vào nội dung an ninh mạng được chia sẻ trên GSM. Kết quả của chúng tôi xác nhận rằng GSM ảnh hưởng tích cực đến cả CSA và IPM.

Cuối cùng, không có sự đồng thuận trong tài liệu về tính hiệu quả của các OPC, đặc biệt là tác động của chúng đối với các EPB. Do đó, chúng tôi điều tra ảnh hưởng trực tiếp của việc tuân thủ OPC đến EPB và tác động gián tiếp của nó thông qua CSA. Phát hiện của chúng tôi chỉ ra rằng việc tuân thủ OPC không có tác động trực tiếp đến EPB; thay vào đó, ảnh hưởng của nó được trung gian bởi CSA.

5.2. Hàm ý quản trị

Điều tra này cung cấp nền tảng vững chắc cho ban quản lý cấp cao của các tổ chức công nhằm xây dựng các giải pháp chiến lược giải quyết những thiếu sót trong quản trị, sử dụng và vận hành hệ thống và mạng máy tính. Các điều tra thực nghiệm chủ yếu tập trung vào khu vực tư nhân, khả năng ứng dụng và chuyển giao các phát hiện cho các tổ chức công vẫn chưa rõ ràng. Các tổ chức công đang dần dần áp dụng số hóa để tăng cường lưu lượng và lưu trữ dữ liệu hoạt động. Tuy nhiên, các OPC hiện tại về quản lý và sử dụng hệ thống máy tính chưa đủ để hỗ trợ những nỗ lực số hóa này, làm tăng nguy cơ mất an toàn thông tin.

Tình trạng không tuân thủ OPC xảy ra trong khu vực công khi các quan chức nhà nước, mặc dù có hiểu biết cơ bản về an ninh mạng, nhưng lại không tuân thủ các tiêu chuẩn của cơ quan. Việc không tuân thủ chính sách không gian mạng, chẳng hạn như sử dụng dữ liệu chưa được xác minh từ ổ USB hoặc truy cập tài nguyên trực tuyến mà không được phép, có thể làm tổn hại đến an ninh mạng và đe dọa dữ liệu hệ thống máy tính đặc quyền của chính phủ. Bằng cách áp dụng luật dựa trên tiêu chuẩn quốc tế mạnh mẽ, các tổ chức chính phủ có thể tăng cường phòng thủ mạng và khuyến khích nhân viên tuân thủ. Điều này sẽ bảo vệ các tài sản quan trọng và tăng cường uy tín của chính phủ.

Việc tuân thủ chính sách của tổ chức cũng ảnh hưởng đến hành vi an ninh mạng của nhân viên. Nghiên cứu này cho thấy việc tuân thủ luật pháp

gián tiếp nâng cao nhận thức về an ninh mạng của nhân viên và sẵn sàng thực hiện các biện pháp phòng ngừa. Các tổ chức phải vượt ra ngoài các chính sách để cải thiện sự tuân thủ và an ninh mạng. Họ nên đầu tư nhiều hơn vào đào tạo, bản tin an ninh mạng và cảnh báo. Những hoạt động này rất cần thiết để phổ biến chính sách hiệu quả và hiểu biết của nhân viên về các mối đe dọa an ninh mạng cũng như các phương pháp hay nhất. Các tổ chức có thể thúc đẩy văn hóa hiểu biết về an ninh mạng và tuân thủ quy định bằng cách thu hút nhân viên thông qua nhiều kênh, điều này sẽ cải thiện quan điểm bảo mật tổng thể của tổ chức.

Xem xét các tác động đáng kể của GSM đối với nhận thức về an ninh mạng và động lực bảo vệ thông tin, các tổ chức chính phủ nên duy trì vai trò tích cực trong việc phổ biến thông tin an ninh mạng một cách nhanh chóng và chính xác thông qua các kênh GSM của họ. Cụ thể, các nền tảng truyền thông xã hội do Chính phủ vận hành đóng một vai trò quan trọng trong việc tăng cường các nỗ lực gần đây của chính phủ tập trung vào việc thúc đẩy an ninh mạng. Thông qua các nền tảng này, các chính phủ có thể nhanh chóng phổ biến thông tin quan trọng liên quan đến các mối đe dọa mạng mới nổi, các biện pháp tốt nhất để đảm bảo an toàn trực tuyến cũng như cập nhật về các chính sách và quy định an ninh mạng. Tương tự, các chính phủ có thể tận dụng hiệu quả khả năng tiếp cận rộng rãi và khả năng tiếp cận thuận tiện của các nền tảng truyền thông xã hội để tương tác trực tiếp với người dân, từ đó nuôi dưỡng ý thức chung về trách nhiệm giải trình và trao quyền trong việc bảo vệ tài sản kỹ thuật số. Hơn nữa, các nền tảng truyền thông xã hội đóng một vai trò quan trọng trong việc tạo điều kiện liên lạc tức thời, cho phép các chính phủ nhanh chóng phổ biến các cảnh báo và cập nhật. Ngược lại, điều này hỗ trợ các cá nhân cảnh giác trước bối cảnh các mối nguy hiểm trên mạng luôn thay đổi. Hơn nữa, các nền tảng này mang đến cơ hội giao tiếp tương tác, cho phép các cá nhân tìm kiếm lời khuyên, trao đổi kiến thức và tham gia vào các

nỗ lực hợp tác nhằm tăng cường khả năng phục hồi an ninh mạng. GSM phục vụ cả việc mở rộng phạm vi của các chương trình nâng cao nhận thức về an ninh mạng, đồng thời nuôi dưỡng một cộng đồng hiểu biết và tham gia nhiều hơn, điều này rất cần thiết để cải thiện tình hình an ninh mạng tổng thể.

5.3. Kết luận

Nghiên cứu này sử dụng khảo sát định lượng và PLS-SEM để xem xét ảnh hưởng của GSM và việc tuân thủ chính sách của tổ chức đối với các khía cạnh hành vi của an ninh mạng. Ngoài ra, nghiên cứu này mở rộng PMT và lý thuyết Tuyên truyền bằng cách giới thiệu hành vi bảo vệ nhân viên như một biến phụ thuộc và xây dựng khung khái niệm tích hợp các hiệu ứng tuyên truyền với GSM. Kết quả cung cấp những hiểu biết mới về sự tương tác phức tạp giữa GSM, nhận thức về an ninh mạng, chính sách của tổ chức, động lực bảo vệ thông tin, ý định tuân thủ, thái độ tuân thủ và hành vi bảo vệ nhân viên. Cụ thể, nhận thức về an ninh mạng tác động tích cực đến cả động lực bảo vệ thông tin và hành vi bảo vệ nhân viên. Hơn nữa, GSM có tác động tích cực đến nhận thức về an ninh mạng và động lực bảo vệ thông tin, trong đó an ninh mạng đóng vai trò trung gian một phần trong mối quan hệ giữa GSM và động lực bảo vệ thông tin. Hơn nữa, tồn tại mối tương quan tích cực đáng kể giữa động lực bảo vệ thông tin và hành vi bảo vệ nhân viên, đồng thời động lực bảo vệ thông tin phần nào làm trung gian cho mối quan hệ giữa nhận thức về an ninh mạng và hành vi bảo vệ nhân viên. Cuối cùng, việc tuân thủ chính sách của tổ chức sẽ nâng cao đáng kể nhận thức về an ninh mạng. Tuy nhiên, việc tuân thủ chính sách của tổ chức không ảnh hưởng trực tiếp đến hành vi bảo vệ nhân viên; thay vào đó, mối quan hệ này hoàn toàn được điều chỉnh bởi nhận thức về an ninh mạng.

5.4. Hạn chế và nghiên cứu trong tương lai

Mặc dù điều tra này cung cấp những hiểu biết mới về lý thuyết và thực tế nhưng nó cũng có những hạn chế nhất định. *Đầu tiên*, việc đo lường EPB bằng bảng câu hỏi định lượng tự báo cáo có thể thiếu giá trị. Việc tự báo cáo có thể không phải là nhân tố dự đoán đáng tin cậy về EPB thực tế của nhân viên vì CSA của họ về EPB bảo mật có thể không phù hợp với thực tế bảo mật thực sự của họ. Điều tra theo chiều dọc sẽ cho phép ghi lại hồ sơ hành vi thực tế chính xác hơn nhưng đòi hỏi nhiều thời gian hơn. *Thứ hai*, các biến kiểm soát như giới tính, chức danh công việc và quy mô tổ chức không được xem xét và sẽ rất có giá trị khi khám phá xem các nhân tố này ảnh hưởng như thế nào đến các mối quan hệ đã thiết lập. *Thứ ba*, việc điều tra các biến số bổ sung ở cấp độ cá nhân, tổ chức và xã hội sẽ cung cấp cái nhìn toàn diện hơn về chủ đề của các EPB.

Chương V. THẢO LUẬN CÁC ĐÓNG GÓP CỦA LUẬN ÁN

Chương này trình bày các đóng góp quan trọng của nghiên cứu vào lý thuyết và thực tiễn quản trị an ninh mạng, đặc biệt trong bối cảnh số hóa ngày càng tăng. Đóng góp về lý thuyết tập trung vào việc mở rộng hiểu biết về lý thuyết nền và cách đánh giá mối đe dọa và chiến lược đối phó ảnh hưởng đến động cơ và hành vi bảo mật của cá nhân.

Thực hiện 10 cuộc phỏng vấn chuyên sâu với các chuyên gia đầu ngành về ANM (*các giáo sư, tiến sĩ hiện là giảng viên đang giảng dạy tại một số trường Đại học tại Việt Nam về CNTT và các Trưởng phòng IT của các Ngân hàng thương mại cổ phần trong và ngoài nước);* Mô tả thông tin người tham gia trả lời phỏng vấn tại bảng 5.1 phần phụ lục; các cuộc thảo luận nhóm với các nhóm hiện là sinh viên thuộc các trường trong Công An nhân dân và trường Đại học Quốc tế; để làm rõ các vấn đề như: thực trạng ANM tại Việt Nam, dự báo tình hình tội phạm ANM trong thời gian tới, hướng nghiên cứu của luận án về ANM, các gợi ý của các chuyên gia đầu ngành về vấn đề đảm bảo ANM tại Việt Nam hiện nay và trong tương lai; kiểm tra, đánh giá trong quá trình xây dựng bộ thang đo.

Kết quả trả lời 10/10 chuyên gia được phỏng vấn, đều đưa ra nhiều khuyến nghị chung trong đó có vấn đề để đảm bảo ANM cho các cơ quan tổ chức cần có chính sách về tài chính để xây dựng nguồn tài chính cho việc thực hiện một số giải pháp về cơ sở hạ tầng CNTT, đào tạo, hay sử dụng đội ngũ cán bộ chuyên trách IT, trong giai đoạn hiện nay và trong tương lai (*hiện nay chưa đồng bộ về cơ sở hạ tầng CNTT, giáo dục, chảy máu chất sám trong việc sử dụng đội ngũ cán bộ chuyên trách IT*).

Từ đó, chúng tôi rút ra các hàm ý trong quản trị sát với tình hình thực tế, giúp các nhà quản lý áp dụng các chiến lược bảo mật thông tin hiệu quả

hơn, thông qua việc tăng cường đào tạo, thiết lập quy trình bảo mật chặt chẽ, và sử dụng công cụ truyền thông để nâng cao CSA trong tổ chức.

I. Đóng góp về lý thuyết

Chương này tóm lược những đóng góp lý thuyết quan trọng về ANM, đặc biệt là việc sử dụng lý thuyết PMT, lý thuyết CT và lý thuyết TPB trong việc giải thích EPB trước các mối đe dọa an ninh mạng. Các điều tra này tập trung vào các khía cạnh sau:

1.1. Bối cảnh và tầm quan trọng của nghiên cứu:

Nghiên cứu bổ sung kiến thức về ảnh hưởng của GSM đến bảo mật thông tin. Mặc dù các hành vi bảo mật thông tin đã được điều tra rộng rãi, tác động của GSM vẫn còn ở giai đoạn sơ khai. Các điều tra trước đây đã xem xét cách bảo vệ con người khỏi các mối đe dọa ANM với sự hỗ trợ của GSM trong các bối cảnh tổ chức và cá nhân. Tuy nhiên, GSM là một nền tảng mạnh mẽ giúp chính phủ và các tổ chức quốc tế nâng cao nhận thức và bảo vệ công chúng khỏi các hiểm họa an ninh mạng.

1.2. Tập trung vào hành vi bảo vệ thực tế:

Các điều tra nhấn mạnh tầm quan trọng của việc nhân viên thực hiện các EPB an ninh thông tin thực tế thay vì chỉ tập trung vào ý định. Các điều tra hiện tại chủ yếu tập trung vào ý định liên quan đến bảo mật, trong khi các điều tra này đo lường toàn diện về ISPC, IPM và EPB. Điều này giúp hiểu rõ hơn về các cơ chế thông qua đó các hành vi bảo vệ được phát triển và thực hiện trong các tổ chức.

1.3. Ảnh hưởng của GSM:

Các điều tra cho thấy GSM có tác động tích cực đến CSA và IPM. GSM ảnh hưởng trực tiếp và gián tiếp đến thái độ tuân thủ và EPB. Đặc biệt, IPM

đóng vai trò trung gian trong mối quan hệ này, chứng tỏ rằng việc sử dụng GSM có thể nâng cao kiến thức CSA và IPM của nhân viên trong việc bảo vệ an ninh thông tin.

1.4. Kết hợp lý thuyết Động lực Bảo vệ và lý thuyết Tuyên truyền:

Các điều tra tích hợp lý thuyết PMT vệ và lý thuyết CT để cung cấp một khung lý thuyết toàn diện về ANM. Lý thuyết PMT đã được mở rộng để bao gồm các hoạt động hữu hình, và lý thuyết CT giúp hiểu rõ hơn về cách các nhân tố này ảnh hưởng đến EPB trong bối cảnh cá nhân và tổ chức.

1.5. Ứng dụng lý thuyết Hành vi Có kế hoạch (TPB):

Các điều tra kết hợp lý thuyết TPB để khám phá mối liên hệ giữa nhận thức, thái độ, ý định và EPB. Lý thuyết TPB giúp làm rõ cách nhận thức CSA và IPM hình thành các ISPC và EPB.

1.6. Ứng dụng trong bối cảnh thực tiễn:

Phát hiện của các điều tra cho thấy việc tuân thủ PP làm tăng CSA, mặc dù tác động đến EPB là gián tiếp. Điều này nhấn mạnh tầm quan trọng của việc tích hợp các chính sách và tài nguyên bảo mật vào văn hóa nơi làm việc để thúc đẩy các hành vi an toàn của nhân viên. Ngoài ra, điều tra còn khám phá ảnh hưởng của việc trau dồi kiến thức thông qua GSM đến các tiền đề của CSA.

1.7. So sánh với các điều tra trước:

Các điều tra này bổ sung kiến thức bằng cách cung cấp nhiều giải thích mang tính lý thuyết về kết quả của việc sử dụng lý thuyết PMT và lý thuyết CT trong các tình huống ANM. Mặc dù các hành vi bảo mật thông tin đã được điều tra rộng rãi liên quan đến tiến bộ công nghệ, nhưng điều tra về các hành

vi này liên quan đến tác động của GMS vẫn còn ở giai đoạn sơ khai. Một số điều tra đã xem xét cách tốt nhất để bảo vệ con người khỏi các hiểm họa an ninh với sự hỗ trợ của GMS, mặc dù nhiều điều tra đã được thực hiện trong bối cảnh tổ chức và bối cảnh cá nhân. Điều này rất quan trọng vì mạng xã hội là nền tảng mạnh mẽ để các chính phủ và tổ chức quốc tế sử dụng nhằm nâng cao kiến thức cho công chúng và đưa ra đề xuất về cách ngăn chặn việc trở thành nạn nhân của tội phạm mạng.

1.8. Kết luận và giá trị đóng góp về mặt lý thuyết của nghiên cứu:

Điều tra cung cấp những hiểu biết sâu sắc về hiệu quả của các sáng kiến an ninh mạng của chính phủ, đánh giá các hành động thực tế thay vì chỉ ý định, và đề xuất các cải tiến trong hoạt động phòng ngừa của nhân viên. Nó củng cố tài liệu về khía cạnh hành vi của an ninh mạng và nhấn mạnh tầm quan trọng của việc tăng cường ý thức và EPB trong các tổ chức chính phủ. Bằng cách tích hợp lý thuyết PMT, lý thuyết CT và lý thuyết TPB, điều tra này cung cấp một khung lý thuyết toàn diện và các gợi ý thực tiễn để nâng cao hiệu quả của các chính sách và chương trình an ninh mạng.

Luận án này không chỉ mở rộng hiểu biết về lý thuyết PMT, lý thuyết CT và lý thuyết TPB mà còn cung cấp các bằng chứng thực tiễn về việc áp dụng chúng trong bối cảnh an ninh mạng, đặc biệt là trong các tổ chức chính phủ tại các nước đang phát triển như Việt Nam.

II. Đóng góp về hàm ý quản trị

Bên cạnh những đóng góp về mặt lý thuyết, luận án cũng góp phần quan trọng trong việc đưa ra những hàm ý quản trị liên quan đến bảo mật thông tin và anh toàn thông tin mạng. Những hàm ý quản trị được rút ra từ ba bài báo liên quan đến điều tra về ANM và cung cấp những khuyến nghị cụ thể cho các nhà quản lý và chuyên gia trong lĩnh vực này. Những phát hiện nhấn mạnh

tầm quan trọng của việc bảo vệ ANM trong bối cảnh chuyển đổi kỹ thuật số và cách các tổ chức có thể áp dụng để củng cố hiệu quả bảo mật thông tin.

2.1. Tầm Quan Trọng của An ninh mạng trong Chuyển đổi Kỹ thuật số

Các điều tra của chúng tôi nhấn mạnh tầm quan trọng của ANM trong bối cảnh chuyển đổi kỹ thuật số. Các nhà điều hành cần chú trọng đến các mối lo ngại về an ninh mạng liên quan đến làm việc từ xa, đồng thời tăng cường năng suất nhóm. Các chuyên gia cần hiểu rõ vai trò của truyền thông xã hội trong việc giảm thiểu rủi ro an ninh mạng, cũng như tầm quan trọng của việc bảo vệ cá nhân. Các biện pháp bảo vệ cần được áp dụng như quy trình đăng nhập phức tạp và sử dụng trình duyệt website an toàn.

2.2. Ảnh Hưởng của Đánh Giá Mối Đe Dọa và Chiến Lược Đối Phó

Bằng chứng điều tra thực nghiệm cho thấy thái độ và động cơ của người dùng đối với các biện pháp bảo mật bị ảnh hưởng bởi đánh giá của họ về mối đe dọa và chiến lược đối phó. Chính phủ và tổ chức nên cung cấp chương trình đào tạo bảo mật thông tin nhằm tăng cường khả năng đánh giá rủi ro và áp dụng biện pháp khắc phục. Các chiến dịch giáo dục và thông tin cần liên tục được thực hiện để nâng cao nhận thức CSA và hiệu quả trong việc đối phó với các vấn đề bảo mật.

2.3. Tác Động của GSM Đến Hành Vi Bảo mật Thông tin

Phát hiện của chúng tôi cho thấy GSM có tác động đáng kể đến hành vi bảo mật thông tin. Chính phủ nên mở rộng sự tham gia vào việc phổ biến thông tin chính xác về GSM, đảm bảo rằng các thông điệp được soạn thảo cẩn thận. Điều này giúp nâng cao nhận thức về an toàn thông tin và khuyến khích các biện pháp bảo vệ.

2.4. Cải Thiện Thái Độ và Động Lực Bảo vệ An ninh

Thái độ và động lực tích cực có thể cải thiện các hành vi bảo vệ an ninh. Nhân viên cần nhận thức rằng bảo vệ an ninh mạng là nhiệm vụ chung của toàn tổ chức. Các tổ chức nên nhấn mạnh tầm quan trọng của các biện pháp phòng ngừa ANM và khuyến khích nhân viên tham gia vào các hoạt động bảo mật thông qua phần thưởng và thăng tiến nghề nghiệp.

2.5. Khuyến nghị Cho Các Nhà Quản Lý

Xây dựng Khuôn khổ Quản trị: Nhà quản lý cần thiết kế và phổ biến các hướng dẫn về ANM, đồng thời tiến hành các chiến dịch giáo dục để nâng cao hiểu biết của tổ chức về bảo mật thông tin.

Đào tạo và CSA: Các chương trình đào tạo về bảo mật cần bao gồm các ví dụ cụ thể về vi phạm bảo mật và các biện pháp phòng ngừa. Khuyến khích trao đổi kiến thức và kinh nghiệm xử lý rủi ro mạng.

Nhận Thức Về Mối Đe Dọa: Nhân viên cần hiểu rõ các mối đe dọa mạng và lợi ích của các biện pháp bảo vệ. Sự tham gia của quản lý cấp cao trong lập kế hoạch chiến lược là cần thiết để thuyết phục nhân viên về tầm quan trọng của an ninh thông tin.

2.6. Tăng Cường Tuân Thủ Chính sách

Việc tuân thủ chính sách an ninh mạng là nhân tố quan trọng ảnh hưởng đến EPB. Các tổ chức cần đầu tư vào đào tạo và các chiến dịch nâng cao nhận thức để phổ biến chính sách hiệu quả và nâng cao CSA. Chính phủ nên duy trì vai trò tích cực trong việc phổ biến thông tin ANM thông qua các kênh GSM, đảm bảo thông tin được truyền đạt nhanh chóng và chính xác.

Tóm lại, luận án này cung cấp cơ sở để các tổ chức xây dựng các giải pháp chiến lược, tăng cường quản trị và bảo vệ hệ thống mạng. Tăng cường đào tạo, nâng cao nhận thức, và xây dựng môi trường tuân thủ chính sách là

những yếu tố then chốt để cải thiện an ninh mạng trong bối cảnh kỹ thuật số hiện nay.

Chương VI. KẾT LUẬN VÀ KIẾN NGHỊ

1. Kết luận

Việc chuyển đổi kỹ thuật số đã cung cấp cho các quan chức chính phủ các kênh hiệu quả để giao tiếp với công chúng, đồng thời gây ra những lo ngại đáng kể về an ninh cho bất kỳ tổ chức nào. Điều tra của chúng tôi tập trung vào cách các hành vi bảo vệ an ninh thông tin được hình thành dựa trên ảnh hưởng của các nền tảng GSM, thái độ bảo mật thông tin và IPM. Để hiểu rõ vai trò của GSM trong việc tác động đến hành vi bảo mật thông tin của người dùng, chúng tôi sử dụng lý thuyết CT và lý PMT làm khung lý thuyết.

Dữ liệu từ khảo sát nhân viên Việt Nam tham gia GSM cho thấy rằng sự tham gia của người dùng vào GSM có tác động tích cực đến việc tuân thủ an ninh mạng thông qua PV và RE. Tuy nhiên, lại có tác động tiêu cực thông qua sự tự tin quá mức SE. Ngoài ra, ATT có tác động mạnh mẽ hơn đến EPB thông qua các nhân tố tác động trung gian so với tác động trực tiếp của nó. Những phát hiện này làm cơ sở để khuyến khích việc điều tra sâu hơn trong thực tiễn quản lý GSM và bảo mật thông tin, đồng thời cung cấp những hiểu biết thực tế cho các nhà quản lý.

Tiếp theo, điều tra phân tích tác động của CSA đến nhân viên tại các doanh nghiệp ở Việt Nam, nhấn mạnh tầm quan trọng của việc tuân thủ các quy định bảo mật và hoạt động bảo vệ tài sản thông tin của công ty. Chúng tôi phát triển một mô hình kết hợp lý thuyết PMT và lý thuyết TPB để xác định xu hướng tuân thủ hệ thống bảo mật thông tin của nhân viên. Kết quả cho thấy, việc nâng cao các khuôn khổ lý thuyết này giúp cung cấp sự hiểu biết toàn diện về yếu tố con người trong bảo mật thông tin và vai trò của quản trị thể chế.

Thông qua phương pháp khảo sát định lượng và phân tích mô hình cấu trúc PLS-SEM, điều tra mở rộng PMT và lý thuyết CT bằng cách giới thiệu

EPB như một biến phụ thuộc. Kết quả cho thấy CSA tác động tích cực đến IPM và EPB. GSM cũng có tác động tích cực đến CSA và IPM, trong đó CSA đóng vai trò trung gian hòa giải một phần trong mối quan hệ này. Hơn nữa, tồn tại mối tương quan tích cực giữa IPM và EPB, với IPM làm trung gian cho mối quan hệ giữa CSA và EPB.

Cuối cùng, việc tuân thủ PP nâng cao CSA, nhưng không ảnh hưởng trực tiếp đến EPB. Thay vào đó, mối quan hệ này hoàn toàn được điều chỉnh bởi CSA. Điều tra này cung cấp cơ sở cho các tổ chức xây dựng các giải pháp chiến lược nhằm tăng cường quản trị và bảo vệ hệ thống thông tin trong bối cảnh chuyển đổi kỹ thuật số.

Nhìn chung, kết quả của điều tra nhấn mạnh tầm quan trọng của việc nâng cao CSA và IPM trong các tổ chức. Các phát hiện khuyến nghị các nhà quản lý cần chú trọng vào việc giáo dục và đào tạo nhân viên, đồng thời xây dựng các chính sách bảo mật hiệu quả nhằm bảo vệ tài sản thông tin và duy trì an ninh mạng.

2. Kiến nghị

Trên cơ sở kết quả điều tra của ba bài báo và kết hợp với phỏng vấn chuyên gia, chúng tôi mạnh dạn đề xuất các kiến nghị sau ở góc độ vay trò quan trọng của Chính phủ trong việc xây dựng chính sách phát triển an toàn thông tin nhằm giảm thiểu những nguy cơ mất an toàn thông tin và đảm bảo ANM. Một số kiến nghị cụ thể:

- Chính phủ cần ban hành những chính sách phát triển về Giáo dục, tuyên truyền về ANM cũng như các quy định, quy trình chung về đảm bảo ANM trong việc xây dựng, quản lý, sử dụng, khai thác hệ thống công nghệ thông tin toàn diện về mọi mặt và trên các lĩnh vực, ngành nghề.
- Thông qua giáo dục giúp cho các nhân viên và người dân có kiến thức về an toàn thông tin, ANM để tự bảo vệ bản thân trước những rủi ro về

ANM; thậm trí thông qua cá nhân họ còn tuyên truyền sâu rộng về kiến thức ANM cho người thân, lên án những hành vi có nguy cơ dẫn đến mất an toàn thông tin trong cơ quan mình, hay thực hiện nghiêm các khuyến cáo, quy đinh về ANM do cơ quan tổ chức của họ đã ban hành và của Cục Khoa Học Công Nghệ về vấn đề bảo đảm ANM *(việc giáo dục cho các nhân viên đang làm việc trong khu vực công nên cần duy trì thường xuyên để giúp nhân viên họ thường xuyên cập nhật kiến thức, cập nhật tình hình ANM và kinh nghiệm thực hành).*

- Các quy định Pháp luật, Nghị định, Thông tư về an toàn thông tin, ANM phải thường xuyên bổ sung thêm các quy định mới để ngày càng chặt chẽ hơn và thống nhất, toàn diện trên mọi khía cạnh ANM để ngăn chặn hay sử lý nghiêm các hành vi vi phạm ANM (*hiện nay các thông tư, nghị định cũng như Luật ANM hiện nay quy định chưa chặt trẽ cũng như chưa đầy đủ, còn chồng chéo hay chưa đủ mạnh và toàn diện về mặt quản lý trên mọi góc độ, khía cạnh để đảm bảo an toàn thông tin – ANM*).
- Chính phủ cần phải củng cố, bổ sung Luật ANM hiện hành để thực hiện quản lý nhà nước toàn diện về mọi mặt, trên các lĩnh vực, ngành nghề về ANM để thống nhất trong việc xử lý, ngăn chặn các loại tội phạm mới phát sinh do việc quản lý ANM chưa tốt, chưa kịp thời, nhóm TPCN ngày nay rất đa dạng và khó quản lý *(do việc quản lý của nhà nước còn lỏng lẻo hiện nay chưa bắt kịp xu thế phát triển của quốc tế nên nhóm tội phạm sử dụng công nghệ cao ANM ngày càng đa dạng và nhiều).*
- Chính phủ cần giao việc bảo đảm ANM cho một cơ quan đơn vị nhất định để chủ trì việc ban hành hay kiểm tra, thực thi các quy định, thông tư, Nghị định của Pháp luật để đảm bảo an toàn ANM cho Quốc gia (*hiện nay các quy định còn chồng chéo, chưa cụ thể, cũng như việc giao quyền cho cơ quan ban ngành chủ trì việc đề xuất, xây dựng, ban hành các quy định để đảm bảo ANM chưa cụ thể, chưa gắn trách nhiệm cho cơ quan cụ thể nên dẫn đến việc đùn đẩy trách nhiệm hay chậm trễ trong việc xây dựng hệ thống Pháp*

luật cũng như ban hành, triển khai biện pháp phòng chống các hành vi vi phạm an toàn thông tin – ANM tại Việt Nam hiện nay).

Ngoài ra, chính phủ cần xây dựng, hoạch định chiến lược hợp tác Quốc tế với các quốc gia về công tác đào tạo, phòng chống tội phạm xâm phạm ANM, cụ thể:

- Hợp tác Quốc tế trong công tác phòng ngừa, đấu tranh, ngăn chặn tội phạm ANM tấn công vào hệ thống mạng lưới công nghệ thông tin nhằm vô hiệu hóa hệ thống máy tính *(thường xuyên cập nhật các phương thức, thủ đoạn hoạt động của tội phạm xâm phạm ANM, hay các lỗ hổng trong công nghệ thông tin bị các Hacker xâm phạm ANM; cách thức chống lại những phương thức, thủ đoạn cũng như đấu tranh với loại tội phạm này mà Quốc tế khuyến cáo)*.
- Hợp tác Quốc tế trong công tác giáo dục, đào tạo nguồn nhân lực.
- Hợp tác Quốc tế trong sản xuất công nghệ thông tin kể cả phần cứng và phần mềm để sử dụng trong các cơ quan trọng yếu hay trong tương lai sử dụng đồng bộ trên toàn lãnh thổ để đảm bảo an toàn thông tin – ANM *(phấn đấu trong tương lai Quốc gia sản xuất và sử dụng công nghệ sạch, tránh nguy cơ tiềm ẩn về công nghệ rễ bị mất an toàn thông tin ANM)*.

Vấn đề tài chính rất quan trọng để thực thi các vấn đề an ninh mạng được đồng bộ và hiệu quả trên phạm vi quốc gia và vùng lãnh thổ, chính phủ cần làm tốt một số vấn đề sau:

- Chính phủ cần tạo nguồn ngân sách, chiến lược phát triển cho việc đồng bộ hóa cơ sở hạ tầng công nghệ thông tin, giáo dục, và thu hút sử dụng nguồn lực lao động có trình độ cao trong lĩnh vực CNTT và ANM *(hiện nay vấn đề phân bổ ngân sách nhà nước cho việc phát triển nguồn nhân lực cũng như đầu tư phát triển cơ sở hạ tầng công nghệ thông tin còn ít và chưa thật hiệu quả),* hiện nay tình trạng phân bổ ngân sách không đồng đều và chưa thật hiệu quả do đội ngũ cán bộ làm công tác trình độ chuyên môn cao còn ít

dẫn đến hiệu quả phòng chống ANM còn yếu chưa theo kịp với sự phát triển của xã hội.

- Chính phủ tạo cơ chế đặc thù ưu tiên ngân sách, tài chính cho các ngành nghề trong lĩnh vực nghiên cứu cũng như sản xuất công nghệ thông tin phục vụ việc bảo đảm an ninh mạng của quốc gia (xây dựng trung tâm nghiên cứu, chính sách miễn thuế hay giảm lãi suất huy động vốn ưu tiên cho nhóm ngành nghề sản xuất công nghệ thông tin),
- Chính phủ cần chính sách phát triển đa dạng các kênh truyền thông của Chính phủ để người dân dễ dàng tiếp cận nhằm nâng cao nhận thức cho người dân về ANM *(cần chi ngân sách nhà nước hay tư nhân hóa cho việc đổi mới các kênh truyền thông của Chính phủ)* như cần có những video clip cho việc tuyên truyền hay sử dụng những nhân vật có ảnh hưởng lớn trên không gian mạng để tuyên truyền, thông cáo những vấn đề mang tính cấp bách về an toàn thông tin – ANM.

- Chính phủ làm tốt được những chính sách đã và sẽ ban hành trong tương lai. Làm được điều này sẽ giảm thiểu tối đa việc mất an toàn thông tin, ANM trên phạm toàn Quốc gia và vùng lãnh thổ đảm bảo phát triển nền kinh tế đột phá lực lượng sản xuất trên nền tảng trình độ khoa học – công nghệ ngày càng cao, hòa nhập Quốc tế công nghệ 4.0; quản lý và điều hành sự phát triển kinh tế, xã hội đúng định hướng *(từ đó cũng đã tác động ý định phải tuân thủ các chính sách, quy định về bảo mật thông tin và đảm bảo ANM của các nhân viên đang làm việc trong khu vực công nên họ đã có hành vi tự bảo vệ bản thân mình trước những nguy cơ mất an toàn thông tin và ANM)*.

3. Hạn chế và khuyến nghị các nghiên cứu trong tương lai

Mặc dù điều tra này đưa ra những quan điểm mới và hữu ích về cả lý thuyết và thực tiễn nhưng vẫn có một số hạn chế nhưng chúng đưa ra những hướng nghiên cứu tiếp theo. *Đầu tiên*, chúng tôi chỉ thu thập thông tin từ các nền tảng truyền thông xã hội nổi tiếng ở một quốc gia. Thiết kế của những nền

tảng này và văn hóa dân tộc có thể làm sai lệch những phát hiện của chúng tôi. Để tăng tính khái quát cho nghiên cứu của chúng tôi, nghiên cứu trong tương lai có thể sử dụng cách tiếp cận đa văn hóa hoặc đa nền tảng. *Thứ hai*, mặc dù một phần đáng kể của phương sai trong biến phụ thuộc được giải thích bằng mô hình của chúng tôi, một số biến quan trọng khác, chẳng hạn như nhận thức về an ninh và chuẩn mực xã hội, không được tính đến. Để nâng cao hơn nữa sự hiểu biết về quản lý GSM và bảo mật thông tin người dùng, các cuộc điều tra trong tương lai có thể kết hợp các yếu tố này. *Thứ ba*, chúng tôi không kiểm tra xem liệu các yếu tố như tính cách, giới tính, trình độ và tình trạng kinh tế xã hội có thể đóng vai trò là yếu tố điều tiết hay không. Những người điều hành tiềm năng này có thể làm sáng tỏ hơn về hành vi bảo mật thông tin của mọi người. Vì lý do đó, nghiên cứu trong tương lai nên xem xét những tác động điều tiết này.

Điều tra này cung cấp những hiểu biết mới về lý thuyết và thực tiễn nhưng nó cũng có những hạn chế nhất định. *Đầu tiên*, việc đo lường hành vi bảo vệ nhân viên bằng bảng câu hỏi định lượng tự báo cáo có thể thiếu giá trị. Việc tự báo cáo có thể không phải là yếu tố dự đoán đáng tin cậy về hành vi thực tế của nhân viên vì nhận thức của họ về hành vi bảo mật có thể không phù hợp với thực tiễn bảo mật thực sự của họ. Nghiên cứu theo chiều dọc sẽ cho phép ghi lại hồ sơ hành vi thực tế chính xác hơn nhưng đòi hỏi nhiều thời gian hơn. *Thứ hai*, việc điều tra các biến số bổ sung ở cấp độ cá nhân, tổ chức và xã hội sẽ cung cấp cái nhìn toàn diện hơn về tiền đề của các hành vi bảo vệ của nhân viên