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

TRẦN VĂN DIỄN

PPMIU22002

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

DANH MỤC CÔNG BỐ KHOA HỌC

Chuyên ngành: Quản lý công

Mã số: 9340403

NGƯỜI HƯỚNG DẪN KHOA HỌC:

PGS. TS Nguyễn Văn Phương

TP. HỒ CHÍ MINH, NĂM 2024

Bài báo được đăng trên tạp chí Quốc tế thuộc danh mục Scopus

TT	**Tên tác giả, tên bài viết, tên tạp chí và số của tạp chí, trang đăng bài viết, năm xuất bản**	**Sản phẩm của đề tài/ dự án** *(chỉ ghi mã số)*	**Số hiệu ISSN**	**Điểm IF**	**Xếp hạng** (Q1, Q2, Q3, Q4)
01	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.	2023	15587894, 15592243	4.03	Scopus Q1.

02	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.	2024	19348835	5.28	Scopus Q2.
03	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.	2024	15587894, 15592243	4.03	Scopus Q1.

04	Van Tran, D., Van Nguyen, P., Dinh, N. T. T., Huynh, T. N., & Van Ma, K. (2024). EXPLORING THE IMPACT OF SOCIAL CAPITAL ON BUSINESS PERFORMANCE: THE ROLE OF DYNAMIC CAPABILITIES, OPEN INNOVATION AND GOVERNMENT SUPPORT. *Journal of Open Innovation: Technology, Market, and Complexity*, 100416.	2024	21998531	6.82	Scopus Q1.

Exploring the influence of government social media on cybersecurity compliance: employee attitudes, motivation and behaviors

Dien Van Tran, Phuong Van Nguyen, Anh Thi Chau Nguyen, Demetris Vrontis and

Phuong Uyen Dinh

Abstract

Purpose - *This study aims to investigate the impact of employees' engagement in government social media (GSM) on their cybersecurity compliance attitude, protection motivation and protective behavior, thereby contributing to effective cybersecurity practices at organizations.*

Design/methodology/approach - *A quantitative cross-sectional field survey was conducted to collect primary data in big cities and large provinces in Vietnam. The final data set of 323 responses was analyzed using the partial least squares-structural equation modeling approach to interpret the results and test research hypotheses.*

Findings - *Engagement in GSM positively influences employees' cybersecurity compliance attitude (ATT). Perceived threat vulnerability and response efficacy also contribute to a positive compliance attitude, although self-efficacy has a negative impact. Moreover, the cybersecurity compliance ATT significantly explains the information protection motivation, which in turn influences employee protective behaviors. However, the relationship between compliance attitude and protective behaviors is weak, unlike previous studies that found a strong correlation.*

Originality/value - *Although recent studies have explored specific information security practices in corporate and home contexts, the influence of GSM on individuals' cybersecurity behaviors has received limited attention because of its novelty. This study contributes to the existing body of knowledge by investigating the impact of GSM on cybersecurity behaviors. This study provides significant contributions to understanding social media's effects of social media on individuals' cultivation processes, by expanding upon the protective motivation theory and cultivation theory. The results lead to practical suggestions for organizational managers and policymakers so that they can enhance their understanding of the importance of cybersecurity, encourage the implementation of self-defense strategies and highlight the significance of threat and coping evaluations in influencing attitudes and motivations.*

Keywords *Cultivation theory, Government social media, Information protective behaviors, Information security, Protection motivation theory*

Paper type *Research paper*

1. Introduction

The prevalence of hostile cyberattacks is increasing because of the rapid evolution in digital technology, which heightens the need to counter cybersecurity threats (Harris and Patten, 2014; He, 2012, 2013; Perez-Moron, 2022). Several widespread cyberattacks have used malware, a kind of pernicious software to infiltrate a network, enabling those who spread it to extort payment from that network's owner or otherwise damage that network. Another common method is phishing, in which deceitful electronic messages are sent to unwitting users to obtain sensitive information to which the sender is not entitled. A third method is man-in-the-middle attacks, in which transactional data exchanged between two parties via public networks is intercepted and pilfered by a third party. Robust information security measures must be used to safeguard critical corporate data stored in these networks (Zhang *et al.*, 2017). Because of technological advances, states and international organizations have increasingly relied on social media platforms to share information and give advice on how to stop these major cybersecurity events (Beaunoyer *etal.*, 2020; Chen *etal.*, 2020; Farooq *etal.*, 2020).

Previous studies have concluded that social media can be important for disseminating warnings (Beaunoyer *et al.*, 2020; Chen *et al.*, 2020; Farooq *et al.*, 2020; Guo *et al.*, 2021). However, the literature on government social media (GSM) - that is, the use of social media by a government - is still in its infancy. The majority of current research focuses on determining why people use GSM (Chen *et al.*, 2020; Guo *et al.*, 2021; Nguyen *et al.*, 2023) or the messaging strategy used in GSM (Chatterjee *et al.*, 2021; Lee and Cho, 2018; Li *et al.*, 2022). In particular, few empirical studies investigate the impact of engagement in GSM on behavioral outcomes. In addition, previous research relies primarily on data obtained from internet users and private social media companies on various social network platforms, rather than sourcing information directly from official GSM to individual users.

In addition, many researchers have shown that both organizations (Anderson and Agarwal, 2010; Johnston *et al.*, 2019; Johnston and Warkentin, 2010; Warkentin *et al.*, 2016) and households (Liang and Xue, 2010; Martens *et al.*, 2019; Tu *et al.*, 2015) take specific information security measures. Nevertheless, it is hard to determine the effect of GSM on these protective behaviors. Information security behavior has received a lot of research attention, but with inconsistent results, in part because the studies do not take attitude and drive into account (Ma, 2022). So, to ensure that the security measures taken to protect various systems are comprehensive, we examine the effect of people's attitudes and motivations on their cybersecurity practices.

Because of increasing access to the internet, the complexity and frequency of cyberattacks have discernibly escalated. The perpetuation of this kind of harmful activity has had considerable and widespread negative effects, encompassing firms, entire industries and even national governments. As a result, governments have implemented specific measures aimed at safeguarding networks related to national security. The objective is to strengthen the legal framework pertaining to network information security to ensure the robust protection of critical national defense information. To do so, governments must prioritize an assessment of the capacity and operational experience of those overseeing the networks. Furthermore, implementation of a comprehensive regulatory framework is crucial for efficient governance of network information security, primarily to minimize the risks and combat the threats in cyberspace. On June 12, 2018, Vietnam's Congress approved the Cyber Security Law, which took effect on January 1, 2019 . This Law governs operations aimed at ensuring social order and safety in cyberspace, as well as the responsibilities of related agencies, organizations and individuals. However, it is imperative to do further research and enhance this legislation to ensure the safety of individuals and organizations when using the internet and online transactions.

To address the gap in the literature, our study uses the protection motivation theory (PMT) (Johnston and Warkentin, 2010) and the cultivation theory (Gerbner *et al.*, 2009; Gerbner and Gross, 1976; Hermann *et al.*, 2020). We build on these theories by incorporating the compliance attitude and protection motivation as precursor factors, so as to gain a comprehensive understanding of the drivers of employee protective behaviors (EPB). The study is based on responses to the following research questions:

RQ1. How does engagement in GSM by a firm's employees influence their attitude toward compliance in cybersecurity measures?

RQ2. What is the relationship between these employees' attitudes toward compliance, protection motivation and protective behavior?

The findings of this study make significant contributions to practitioners by illuminating the relationships among engagement in GSM, attitude toward compliance, protection motivation and protective conduct. Our research offers professionals valuable insights into the possible impact of social media in facilitating the distribution of information to address and reduce cybersecurity concerns. Our study further emphasizes the importance of self-defense for individual users. Moreover, it is advisable for government agencies and other businesses to implement information security training programs that have been customized to address security concerns. The primary objective of these programs should be to enhance the competencies of individuals, encompassing personnel, in proficiently assessing prospective security hazards and implementing suitable countermeasures. The endorsement of several crucial activities is vital, including the implementation of regular campaigns designed to educate employees on the need of minimizing their online footprint, the promotion of employee safety and the detection of internal threats.

The remainder of the study is organized as follows. The literature review and theoretical framework are shown in Section 2. The research model and the proposed hypotheses are discussed in Section 3. The methodology used to answer the suggested research questions is described in Section 4. The research results and discussion are presented in Section 5. Section 6 offers our research implications, conclusions and limitations.

2. Literature review

2.1 Protection motivation theory

PMT is the most frequently used theory in behavioral security studies (Wall and Warkentin, 2019), as it explains how people interpret danger and decide which defenses to use in protective behaviors. According to PMT, two processes underlie how people react to risks and defend themselves: threat appraisal and coping appraisal. The threat is evaluated using the threat appraisal method, which is broken down further into an evaluation of perceived severity and PV (PV) (Witte *et al*., 2010). However, some previous studies emphasize the overlap between perceived severity and susceptibility (Ameen *et al*., 2021; Ifinedo, 2012). In line with these studies, we incorporate PV into the research model when predicting PMT in the threat appraisal process.

In coping appraisal, people evaluate potential responses to hazards concurrently with their assessment of the risks. This process, which assesses a person's propensity for taking the protective measures necessary for reducing a threat, can be broken down further into response efficacy (RE), self-efficacy (SE) and response costs (Johnston and Warkentin, 2010; Witte et *al*., 2010). Following Martens et *al*. (2019), this study does not consider response cost because it is ambiguous and measuring it is challenging (Warkentin et *al*., 2011).

2.2 Cultivation theory

Cultivation theory is a theory of communication introduced in the 1970s by George Gerbner and his colleagues to explain changes in viewer behavior due to exposure to mass media (Gerbner *etal*., 2009; Hermann *etal*., 2020). Cultivation is defined as viewers' perception of social reality due to exposure to information via social media (Gerbner *etal*., 2009). In other words, constant social media exposure helps people develop and maintain a unique set of beliefs (Cheng *etal*., 2016). The cultivation effect of social media might change how viewers interpret the world, depending on information presented on social media, rather than in reality (Hermann *et al*., 2020). Social media use two cognitive processes to sway public opinion during the cultivation phase: mainstreaming and resonance (Tang *et al*., 2021).

When individuals' viewpoints align with the content that they obtain from social media platforms, resonance is intensified, reinforcing the nurturing effect.

2.3 Government social media

The use of social media in government is one of the key trends in the study and practice of e-government (i.e. digitization in government functions) in recent years (Criado *etal*, 2013). An official GSM account, as defined by this study, is an online public profile created and maintained by a government agency on social media to disseminate information and collect feedback from users (Medaglia and Zhu, 2017). GSM engagement or participation is defined as interaction with messages (e.g. reading, commenting on or responding to and sharing posts) posted by GSM accounts by users or followers of those accounts (Guo *etal*., 2021). Social media is characterized by an ability to reduce or eliminate barriers to communication among individuals (or between individuals and institutional representatives) and facilitate interaction between citizens and their government. In the literature, this ability is acknowledged to be a significant technological tool for governments to use for communicating warnings and other kinds of information to the public. Moreover, its cultivation effect enhances the situational awareness and knowledge of individuals, further bolstering its potential for broadcasting important information (Beaunoyer *etal*., 2020; Chen et *al*., 2020; Farooq et *al*., 2020; Guo et *al*, 2021). However, few empirical studies have examined the effect of engagement in GSM on citizens' behaviors.

2.4 Information security attitude, motivation and behaviors

In the context of information security, we define EPB as the actions they take to avoid information security problems (Martens et *al*., 2019; Tu et *al*., 2015). Moreover, a cybersecurity compliance attitude (ATT) is defined as a positive view about compliance with information security policies (Wong et *al*., 2022). Many studies concentrate on how to ensure EPB and a cybersecurity compliance ATT (Anderson and Agarwal, 2010; Ifinedo, 2012; Siponen *et al*., 2014), and others examine whether an employee forms an intention to violate an information security policy (Siponen and Vance, 2010) or to abuse information systems. Still other prior research focuses on individual contexts (Liang and Xue, 2010; Martens *etal*., 2019; Tu *et al*., 2015) and organizational contexts (Johnston and Warkentin, 2010; Nair *et al*., 2019; Warkentin *et al*., 2016). However, attitudes toward compliance, protection motivation and engagement in protective behaviors by employees have received little attention.

3. Hypotheses development

3.1 Government social media, perceived vulnerability, self-efficacy and response efficacy

PV is people's estimation of the likelihood of harm or a view about their susceptibility to being victims of a specific threat (Johnston and Warkentin, 2010; Witte *etal*., 2010). SE is a person's self-evaluation of the ability to engage in protective conduct or of whether a person has the knowledge, abilities and resources necessary to perform a task responsibly (Maddux and Rogers, 1983). RE means people's level of confidence that a suggested solution will successfully mitigate the degree of threat to them (Tang *etal*., 2021).

Previous research on cultivation theory reveals that the use of social media by individuals has a significant impact on their attitudes and perceptions (Albashrawi *etal*., 2022; Gerbner *etal*., 2009; Gerbner and Gross, 1976; Hermann *etal*., 2020). People who spend more time on social media are more likely to perceive that the real world is similar to what they see and hear on social media. The impacts of social media consumption on the threat appraisal process are well documented (Intravia *et al*., 2017; Kim and Hawkins, 2020; Shah *et al*., 2020). Previous research indicates that, irrespective of the media outlet, greater exposure to information on disasters or crime leads individuals to experience higher levels of anxiousness. This can be attributed to the perception that these individuals themselves, their family or others could experience the events depicted in the media (Intravia *et al*., 2017; Kim and Hawkins, 2020; Shah *etal*., 2020). This study tests the notion that engaging in GSM can be seen as a form of social media consumption behavior. We test the hypothesis that people who engage in activities such as reading, commenting on and sharing security information that originates from GSM are more inclined to have a more compliant attitude and a greater sense of PV. Our first two hypotheses are postulated as follows:

H1. Engagement in GSM is positively associated with a cybersecurity compliance ATT.

H2. Engagement in GSM is positively associated with PV.

In addition to inducing fear or a perceived sense of threat among individuals, social media platforms are also a means of educating users on how to enhance their preparedness for dangers, such as natural disasters (Farooq et *al.*, 2020). According to cultivation theory (CT), people can evaluate the success of using defensive responses using the knowledge that they accumulate from GSM as a foundation, thereby increasing their RE (Tang *et al.*, 2021; Tu *et al.*, 2015). Moreover, people can improve their SE by learning and getting information on threat appraisal on social media (Kim and Hawkins, 2020; Tu *et al.*, 2015). People are more likely to use certain measures confidently when they are more knowledgeable about viable countermeasures to dangers (Tang *et al.*, 2021; Tu *et al.*, 2015). Hence, we hypothesize that employees' confidence in their capacity to mitigate risks is likely to engagement in GSM. Consequently, the following hypotheses are proposed:

H3. Engagement in GSM is positively associated with SE.

H4. Engagement in GSM is positively associated with RE.

3.2 Perceived vulnerability, self-efficacy and response efficacy

The employee's level of familiarity with potential dangers and their ability to manage them might influence their behaviors through the formation of behavioral, normative or control beliefs within the context of security (Bulgurcu *etal.*, 2010). According to PMT, people who believe that they are vulnerable to threats are likely to have a compliance attitude toward information security (Hina *et al.*, 2019). Previous research indicates that people who have knowledge about a potential hazard are more likely to take precautionary measures to avoid becoming victims of that threat (Johnston and Warkentin, 2010). Consequently, their compliance attitudes are positively influenced (Anderson and Agarwal, 2010; Wong *et al.*, 2022). Therefore, we hypothesize that employees who have a heightened feeling of vulnerability demonstrate a more favorable disposition toward expending additional effort to ensure task security. Consequently, the subsequent hypothesis is posited:

H5. PV is positively associated with a cybersecurity compliance ATT.

According to PMT, employees' coping-appraisal responses are contingent upon their belief in their capability to successfully execute tasks, as well as their expectation of their effectiveness (Sharma *et al.*, 2020). SE is used in earlier research to explain people's computer-related attitudes (Crossler *et al.*, 2013; Johnson and Marakas, 2000; Ma, 2022; Wong *et al.*, 2022). However, these empirical investigations have conflicting results. In particular, SE and compliance attitude have a positive association (Anderson and Agarwal, 2010; Johnston and Warkentin, 2010), but other studies state that these factors have different effects on one another (Hooper and Blunt, 2020; Moody *etal.*, 2018). In this study, we investigate the link between SE and compliance further, proposing the following hypothesis:

H6. SE is associated with a cybersecurity compliance ATT.

Based on PMT, prior research indicates that individuals might choose not to engage in protective actions if they perceive a security measure as both simple to install and ineffective (Hanus and Wu, 2016; Johnston and Warkentin, 2010; Wong *et al.*, 2022). In other words, RE positively influences people's attitudes toward adopting suggested individual information security protective behaviors. Other researchers argue that the relationship is insignificant (Siponen *etal.*, 2014). Despite the inconsistent results, this study assumes that employees have a more favorable attitude toward a recommended response if they believe in its efficacy. Consequently, the following hypothesis is proposed:

H7. RE is positively associated with a cybersecurity compliance ATT.

3.3 Compliance attitude, protection motivation and protective behavior

From the PMT perspective, attitude affects employees' intention to follow security regulations and is positively correlated with adherence with organizational information security policies (Siponen *et al.*, 2014). Ma (2022) also finds that a positive attitude toward information security protection positively impacts an employee's protection motivation. Numerous prior studies have similar findings (Ameen *et al.*, 2021; Hina *et al.*, 2019; Ma, 2022; Martens *et al.*, 2019; Safa *et al.*, 2015; Wu, 2020). In line with previous research, we believe that employees with a positive attitude toward protecting the informational assets of their organization have larger information protection motivation (IPM) and more protective behavior. Consequently, the following hypotheses are proposed:

H8. A cybersecurity compliance ATT is positively associated with EPB.

H9. A cybersecurity compliance ATT is positively associated with IPM.

PMT should be expanded to predict behavior because the goal of information security research is to improve EPB, rather than to increase protection intentions (Floyd *etal.*, 2006). In line with this perspective, Liang and Xue (2010) integrate real-life EPB into the testing framework and discover a positive correlation between people who exhibit a higher motivation to engage in information protection and a higher propensity to engage in measures meant to prevent against information security incidents. Other papers confirm similar findings (Lebek *et al.*, 2014; Siponen *et al.*, 2014; Warkentin *et al.*, 2016). In this study, we believe that EPB depends on the motivation to protect information security. Consequently, the following hypothesis is proposed:

H10. A motivation to protect information is positively associated with EPB.

As previously discussed, the relationship among the constructs proposed for this conceptual model is shown in Figure 1. The research model includes engagement in GSM, PV, SE, RE, a cybersecurity compliance ATT, motivation to protect information and EPB. This conceptual model evaluates the relationship between these constructs and is based on our ten hypotheses.

4. Methodology

4.1 Measurement

The survey instrument in this study was created with the use of available literature. All questions in this survey are graded on a seven-point Likert scale, from 1 = "strongly disagree" to 7 = "strongly agree." All the scales measured were adapted from previous studies with minor or major modifications (see Appendix Table A1).

4.2 Data collection

From October 2022 to March 2023, self-administered survey forms were sent to various employees working in big cities and provinces in Vietnam, such as Ho Chi Minh City, Hanoi,

Figure 1 Research model

Dong Nai Province and Binh Duong Province, where at least one social media platform, such as Facebook, Zalo, Viber, YouTube, TikTok and Instagram, is used. Of the 700 questionnaires distributed, 564 were returned, and 323 of them were deemed appropriate for study. The sample size was determined to be sufficient based on Hair *et al.* (2014). Questionnaires that satisfy one of the following conditions are discarded as invalid:

- if all the respondents give the same responses to all the questions (e.g. all 1 or all 7); or
- if respondents finish the survey in less than 2 min (Collier and Sherrell, 2009).

We use a - test to compare the demographic characteristics of the first and last responders, as recommended in prior literature, to rule out any potential nonresponse bias (Collier and Sherrell, 2009; Han *et al.*, 2017). Because we find no discernible differences between the two groups of respondents, we believe that nonresponse bias is not a problem.

4.3 Research method

In this study, the research model was determined through the use of partial least squares- structural equation modeling (PLS-SEM) analysis for several reasons. First, it is better suited for a regression with mediation than other methods. Second, it takes measurement error into account and provides accurate estimates for mediating effects (Chin, 1998b). It is also appropriate for both simple and complex frameworks and does not require an assumption of data normality (Hair et *al.*, 2014). Third, PLS-SEM is considered more suitable than ordinary least squares regressions when there are issues such as missing values or multicollinearity, and the sample size is small. Finally, it is also widely used in the context of information security behavior (Ma, 2022; Wong *etal.*, 2022).

5. Results and discussion

The SmartPLS 4.0 application module was used to investigate the research model. After performing descriptive analyses, we use the two-stage analytical technique (Hair et *al*., 2014).

5.1 Descriptive analysis

Table 1 below describes detailed information on the demographic characteristics of respondents, based on the data collection.

Table 2 displays the mean and standard deviation for each variable. All survey participants were asked to describe their perceptions using a seven-point scale, from 1 (strongly disagree) to 7 (strongly agree). Cybersecurity compliance ATT has the highest score, with an average of 6.283 out of 7.0 and a standard deviation of 1.114. SE has the lowest score, with an average of 5.554 out of 7.0 and a standard deviation of 1.625.

5.2 Measurement model assessment

Convergent and discriminant validity are applied in testing the measurement models. The main variables in this study are assessed using Cronbach's alpha coefficients (construct reliability). Each Cronbach's alpha coefficient in this study is from 0.914 to 0.949, exceeding the threshold value of 0.7 (Kannan and Tan, 2005). Furthermore, all composite reliability (CR) factors have values from 0.946 to 0.964, exceeding suggested value of 0.7 (Gefen *etal*., 2000). As seen in Table 2, construct reliability, therefore, is satisfied because CR and Cronbach's alpha are essentially error-free for each construct.

Using factor loadings, we evaluated indicator reliability. In addition to being captured within the constructs, the conditions are implied by the large loadings observed on corresponding constructs even when associated indicators have a common basis (Hair *etal*., 2014). All the items in Table 2 have factor loadings above the recommended value of 0.7, with the exception of RE10, which was dropped from the scale because of its low loading values.

The study uses average variance extracted values (AVE) as a means to assess the convergent validity. Each AVE has a value from 0.642 to 0.899, above the suggested threshold of 0.50 (Hair, 2011). The findings presented in Table 2 show that all the constructs successfully satisfy the criteria for convergent validity.

5.3 Common method bias

Various researchers have found that full collinearity can be used to identify common method bias (CMB). According to Kock (2015), if the full collinearity value (FCVIF) is less than 3.3, then the data do not have any CMB issues. As shown in Table 2, all the latent constructs in the data have an FCVIF below3.3, indicating the absence of any CMB issues.

Table 1 Demographic characteristics of respondents

Demographic characteristics	*Category*	*No.*	*Percentage (%)*
Gender	Male	239	74.0
	Female	84	26.0
Age	18-35 years	232	71.9
	36-45 years	72	22.3
	Over 45 years	19	5.9
Education	High school	90	27.9
	Undergraduate	180	55.7
	Postgraduate	53	16.4

Years of experience	Less than 3 years	48	14.9
	3 to 5 years	56	17.3
	More than 5 years	219	67.8
Organizational scale	Less than 50 employees	97	30.0
	51 to 100 employees	57	17.6
	More than 100 employees	169	52.4

Source: Created by the authors

Table 2 Descriptive and measurement assessment

Constructs	*Item no.*	*Loadings (> 0.5)*	*Mean*	*SD*	*α (> 0.7)*	*CR(> 0.77)*	*AVE(> 0.5)*	*FCVIF*
Government social media (GSM)	GSM1	0.933	5.922	1.382	0.935	0.958	0.885	2.382
	GSM2	0.964						
	GSM3	0.924						
Perceived threat vulnerability (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						
Self-efficacy (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						
Response efficacy (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	Deleted						
Cybersecurity compliance attitude (ATT)	ATT1	0.942	6.283	1.114	0.944	0.964	0.899	1.911
	ATT2	0.955						
	ATT3	0.948						
Information protection motivation (IPM)	IPM1	0.908	6.114	1.250	0.949	0.961	0.830	2.352
	IPM2	0.891						
	IPM3	0.903						
	IPM4	0.932						
	IPM5	0.921						
Employee protective behaviors (EPB)	EPB1	0.917	5.957	1.401	0.914	0.946	0.854	1.124
	EPB2	0.937						
	EPB3	0.919						

Source: Created by the authors

To evaluate the discriminant validity, we use Fornell-Larcker and heterotrait-monotrait ratios (HTMT) (displayed in Table 3). The square roots of the AVEs on the diagonals are higher than those for correlations among the constructs (corresponding rows and columns), which is typically an indication of strong correlations among constructs and their corresponding indicators (Chin, 1998a, 1998b; Fornell and Larcker, 1981). In addition, when HTMT values are higher

than the threshold of 0.85, significant problems with discriminant validity arise. However, the correlation between the exogenous constructs and every HTMT is lower than 0.85. As a result, the discriminant validity of all constructs is satisfactorily confirmed.

5.4 Structural model assessment

To test the structural models, we use bootstrapping technique calculate the beta *(b)*, R_2 and respective - values for a resampling of 5,000 (Hair *et al.*, 2014). The calculation of R^2 was performed to evaluate the predictive capability of the structural model. The coefficient of determination (R^2) quantifies the proportion of variance in the endogenous variables that can be attributed to the exogenous variable. According to Cohen (1988), the R^2 values of

Table 3 Fornell-Larcker And HTMT results

	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*
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	

Note: The square roots of the AVEs are shown in italic face on the diagonals
Source: Created by the authors

0.75, 0.50 or 0.25 for endogenous latent variables in the structural model can be characterized as significant, moderate or low, correspondingly. The findings derived from Table 4 demonstrate that the R^2 values of the endogenous constructs fall within the designated tolerance range. Consequently, these results indicate that the model has a comparatively elevated level of predictive accuracy overall.

In addition, we assess the significance of the magnitudes of the structural coefficients. Cohen (1988) suggests that a f^2 value of 0.02, 0.15 and 0.35 represents weak, moderate and strong effects, respectively. As presented in Table 4, the effect sizes of the examined associations lie within the strong range, except for weak case when the effect size of the connections between ATT with EPB is equal to 0.002.

5.5 Hypotheses testing

The SEM assessments in Figure 2 and Table 4 show the outcomes of hypothesis testing, which confirms all the hypotheses. Engagement in GSM meaningfully predicts PV, SE, RE and a cybersecurity compliance ATT; all the p-values are less than 0.001, therefore, *H1-H4* are confirmed. These findings are similar to those for PV and RE, both of which meaningfully influence cybersecurity compliance ATTs. Hence, both *H5* and *H7* are also confirmed, and

Table 4 Structural assessment results

Hypothesis	*Relationship*	*Std b*	*t-value*	p-*value*	R^2	f^2	*Result*
H1	GSM → ATT	0.350	13.220	0.000	0.653	0.160	Supported
H2	GSM → PV	0.612	9.291	0.000	0.373	0.600	Supported
H3	GSM → SE	0.679	14.746	0.000	0.459	0.855	Supported
H4	GSM → RE	0.708	13.972	0.000	0.500	1.006	Supported
H5	PV → ATT	0.360	3.656	0.000	0.653	0.154	Supported
H6	SE → ATT	-0.184	2.435	0.015		0.037	Supported
H7	RE → ATT	0.352	3.508	0.000		0.099	Supported
H8	ATT → IPM	0.824	17.001	0.000	0.677	2.109	Supported
H9	IPM → EPB	0.776	10.517	0.000	0.646	0.551	Supported
H10	ATT → EPB	0.035	11.412	0.000		0.002	Supported

Source: Created by theauthors

Figure 2 Testing results

SE meaningfully predicts cybersecurity compliance ATT, so *H6* is confirmed. However, the path is negative, with a -value lower than 0.05, indicating that SE has a negative effect on a cybersecurity compliance ATT. *H8* and *H10* are supported, with p-values less than 0.001, which suggests that a cybersecurity compliance ATT significantly predicts an IPM and EPB. *H9* is supported, as an IPM has a significant effect on EPB.

We estimated the indirect effects to determine: the mediating effects of PV, SE and RE on the relationship between GSM and ATT, and the mediating effect of IPM on the relationship between ATT and EPB (see Table 5). The results indicate that all factors play a partial mediating role in the two relationships.

5.6 Discussions

This research significantly contributes to the field of information security by providing a comprehensive examination of the impact of GSM on employees' attitudes and actions toward information security. It considers several aspects, including attitudes, motivations and behaviors, from a broader perspective, catering to the interests of both information security academics and practitioners. The findings provide strong evidence to support the 10 hypotheses.

Initially, the GSM engagement has positive outcomes in terms of fostering positive attitudes toward cybersecurity compliance. More specifically, it plays a role in fostering positive attitudes among employees toward engaging in protective behaviors. This result is consistent with previous research (Hermann *etal.*, 2020; Yin *etal.*, 2022), which argues that frequent use of social media enhances positive attitudes toward protective behaviors. In

Table 5 Mediating effects

Hypothesis	*Type*	*Estimates*	*t-values*	p-*values*	*Remarks*
H6. GSM → ATT	Direct	0.350	13.220	0.000	Supported
GSM → PV → ATT	Indirect	0.220	3.082	0.002	Complementary (partial mediation)
GSM → SE → ATT	Indirect	-0.125	2.369	0.018	Complementary (partial mediation)
GSM → RE → ATT	Indirect	0.249	3.188	0.001	Complementary (partial mediation)
H10. ATT → EPB	Direct	0.035	11.412	0.000	Supported
ATT → IPM → EPB	Indirect	0.639	9.123	0.000	Complementary (partial mediation)

Source: Created by the authors

addition, engagement in GSM has a positive influence on PV, RE and SE, which implies that the longer that people engage in GSM security-related content, the more vulnerable they feel to the threat of information security risks and

their own SE as well as RE when confronting such risks. Our findings correspond those in with previous research (Intravia *eta.*, 2017; Kim and Hawkins, 2020; Shah *etal.*, 2020; Tang *etal.*, 2021; Tu *etal.*, 2015).

Second, we find that a cybersecurity compliance ATT is positively influenced by PV and RE. These findings are consistent with those in previous studies (Anderson and Agarwal, 2010; Hina *et al.*, 2019; Ifinedo, 2012; Wong *et al.*, 2022). Nevertheless, the empirical findings demonstrate that PV and RE have a positive influence on compliance attitude. Conversely, SE has a negative impact on compliance attitude. This finding implies that people are less inclined to be well disposed to adhering to cybersecurity protocols when they believe that they can execute the prescribed measures and effectively manage potential threats. This pertains specifically to their perceived competence and judgment in addressing the dangers associated with a security breach. This finding contributes to the predominantly mixed results because it is consistent with some studies (Hooper and Blunt, 2020; Moody *etal.*, 2018), but not others (Anderson and Agarwal, 2010; Johnston and Warkentin, 2010).

Finally, we find that an IPM is substantially positively explained by an employee's attitude toward compliance. The relationship between these two dimensions suggests that employees are more motivated to spend extra time and effort protecting information assets when they generally have a more positive attitude toward protective behaviors. This finding aligns with those in prior studies (Hina *et al.*, 2019; Ma, 2022; Martens *et al.*, 2019; Safa *etal.*, 2015; Wu, 2020). In addition, we find that an IPM subsequently has a significant effect on EPB, which is consistent with previous findings (Lebek *etal.*, 2014; Siponen *etal.*, 2014; Warkentin *et al.*, 2016). Specifically, employees with a heightened level of motivation to safeguard information security are more inclined to engage in behaviors that mitigate security risks.

6. Implications and conclusion

6.1 Theoretical contributions

This study adds to the corpus of knowledge by providing many theoretical explanations of the result from using PMT and CT in cybersecurity scenarios. First, even though information security behaviors have been extensively researched in relation to technological advancement, research on these behaviors in relation to the impact of GSM is still in its infancy. Few studies have looked at how best to protect people from security threats with the aid of GSM, although many studies have been conducted in organizational contexts (Johnston and Warkentin, 2010; Warkentin *etal.*, 2016) and individual contexts (Liang and Xue, 2010; Martens *etal.*, 2019; Tu *etal.*, 2015). This is significant because social media are powerful platforms for governments and international organizations to use for enlightening the public and offering suggestions on how to prevent being a victim of cybercrime (Beaunoyer *et al.*, 2020; Chen *et al.*, 2020; Farooq *et al.*, 2020). This study adds to knowledge on the influence of GSM on behavioral information security by examining the cultivation effects of GSM on PMT variables and EPB.

Second, rather than examining actual behavioral change, existing information security studies primarily concentrate on security-related intention. They assert that, although PMT primarily revolves around intentions, it has been effectively expanded to encompass tangible activities. This study demonstrates the significance of employees' implementation of actual information security protective behaviors to enhance these behaviors, as well as in foster compliance attitudes and a protection motivation. The comprehensive measurement of attitudes, motivations and behaviors facilitate deeper comprehension of the mechanisms through which protective behaviors are developed (Floyd *etal.*, 2006).

Third, our paper is a pioneering study on the impact of social media on cultivation effects. In contrast, previous works primarily focus on the cultivation impacts of conventional mass media, such as television and newspapers, on individuals' views and attitudes (Hermann *et al.*, 2020; Tang *et al.*, 2021). In addition to examining the cultivation impacts of social media, our study specifically looks at the consequences of GSM accounts. We find that through PMT elements, GSM has both direct and indirect impacts on followers' attitudes throughout PV, SE and RE. Moreover, IPM plays a partial mediating role in the relationship between ATT and EPB.

Finally, the incorporation of CT into our study expands existing knowledge on PMT, which is examined in prior papers. In contrast to another study (Tu *et al.*, 2015), which emphasizes the importance of evaluating threats and coping mechanisms to implement security measures in organizational systems, this study presents a more sophisticated model that specifically examines the factors that influence individuals' evaluations of threats and coping strategies in a personal context. The data analysis results provide support for all our hypotheses, indicating that PMT and cultivation theory effectively account for responsible conduct. We expand the application of these theories, as they are shown to possess explanatory capabilities within the framework of ongoing research. In addition, they serve as a foundation for estimations regarding key threats and coping strategies.

6.2 Practical contributions

First, the study has many practical implications for professionals in the field. Our findings highlight the importance of cybersecurity in the context of digital transformation. Executives have placed increasing focus on the cybersecurity concerns associated with remote teams, in addition to recognition of the importance of remote team productivity. Our study provides professionals with insights into the potential role of social media in facilitating information dissemination to mitigate cybersecurity risks. Our research further highlights the significance of self-defense for individual users. Hence, it is imperative for practitioners to actively advocate for the adoption of cyber hygiene practices to enhance proactive self-protection measures. Some of these measures include the use of more complex login procedures (credentials and passwords; two-step verification; passkeys), as well as using web browsers that can store passwords, subject to their own master login or password procedures.

Second, empirical evidence substantiates the notion that users' attitudes and motivation to implement security measures are notably impacted by their evaluations of threats and coping strategies. Government agencies and other organizations are recommended to provide information security training programs that specifically target security threats. These programs should aim to strengthen the abilities of individuals, including employees, to effectively evaluate potential security risks and use appropriate remedies. Several important activities, such as launching frequent campaigns aimed at educating employees about minimizing their internet presence, promoting employee safety and detecting internal dangers, are of the utmost importance and should be endorsed. When individuals perceive a higher level of RE, they are more inclined to use successful coping techniques. Consequently, it is imperative for government bodies to distribute communications that promote responsible use of technology and enhance efficiency in addressing issues. During the adoption process, it is imperative for organizations to effectively explain their implementation policies to all employees. To enhance the promotion of protection motivation, companies need to ensure that the measures used are implemented in a precise, organized and simple way. Subsequently, employees will have the capacity to prioritize which methods offer the greatest safeguards in their ongoing effort to manage and mitigate dangers.

Third, our findings further demonstrate the indirectly effect of PMT variables on our dependent variable through engagement in GSM. This suggests that GSM can have a significant impact on the behavior of individuals when it comes to information security as a digital cultivation medium. Government organizations should continually expand their involvement in spreading correct and pertinent information about their GSM. To guarantee the maximum impact, these GSM messages should be carefully crafted and chosen. Information security issues may have a detrimental social impact because threat and coping assessments in organizations are effective. Messages that share relevant examples of serious information security concerns are, therefore, strongly advised. Government organizations should consistently promote the value of information security protection and stress the vulnerability of nonprotective actions when developing messaging.

Finally, creating positive attitudes and motivations that can improve protective behaviors is essential because security breaches are significant and important to enterprises, as shown by our research. Risk management teams and employees are essential players and defenders of cyber resilience because most firms are still in the early stages of their digitization. Employees should be aware that cybersecurity defense is a shared duty among organizational staff and departments. Everyone with an internet connection is affected. To improve their cybersecurity posture, organizations should emphasize the significance and advantages of cybersecurity preventive behaviors.

6.3 Conclusions

The digital transformation has simultaneously provided government officials with effective channels to communicate with the public and raised significant security concerns for any organization. This paper presents novel research that shows how information security protective behaviors are formed based on the influence of GSM, information security attitudes and protection motivation. To investigate the role of GSM in influencing users' information security behaviors toward information security concerns, we specifically use both CT and PMT as theoretical frameworks. We experimentally evaluate our proposed research model and hypotheses by examining data from a survey of Vietnamese employees who engage in GSM. Our research shows that users' engagement in GSM has a positive impact on cybersecurity compliance ATT toward using security measures through PV and RE, but a negative impact through SE. In addition, a cybersecurity compliance ATT has a stronger impact on EPB through an IPM than from its direct impact. Our findings encourage further investigation into GSM management and information security practices and offer practical insights for practitioners.

6.4 Limitations and further studies

Although the study offers new and helpful perspectives on both theory and practice, it has some limitations, but they offer directions for further research. First, we gather information only from well-known social media platforms in a single country. The design of these platforms and the national culture may skew our findings. To increase the generalizability of our study, future research can use a cross-cultural or cross-platform approach. Second, although a significant portion of the variance in our dependent variable is explained by our model, a few other crucial variables, such as security awareness and social norms, are not taken into account. To further advance understanding of GSM management and user information security, future investigations may incorporate these elements. Third, we do not examine whether factors such as personality, gender and socioeconomic status might act as moderating factors. These possible moderators might be able to shed more light on people's information security behaviors. For that reason, future research should examine these moderating effects.

References

Albashrawi, M., Asiri, Y., Binsawad, M. and Alqahtani, L. (2022), "The effect of social media use on empathy and welling: a personality perspective in Saudi Arabia", *Journal of Asia Business Studies*, Vol. 16 No. 2, pp. 406-423, doi: 10.1108/JABS-11-2020-0461.

Ameen, N., Tarhini, A., Shah, M.H., Madichie, N., Paul, J. and Choudrie, J. (2021), "Keeping customers' data secure: a cross-cultural study of cybersecurity compliance among the gen-mobile workforce", *Computers in Human Behavior*, Vol. 114, p. 106531, doi: 10.1016/j.chb.2020.106531.

Anderson, C.L. and Agarwal, R. (2010), "Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions", *MIS Quarterly: Management Information Systems*, Vol. 34 No. 3, pp. 613-643, doi: 10.2307/25750694.

Beaunoyer, E., Dupéré, S. and Guitton, M.J. (2020), "COVID-19 and digital inequalities: reciprocal impacts and mitigation strategies", *Computers in Human Behavior*, Vol. 111, p. 106424, doi: 10.1016/J. CHB.2020.106424.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly: Management Information Systems*, Vol. 34 No. 3, pp. 523-548, doi: 10.2307/25750690.

Chatterjee, S., Chaudhuri, R., Vrontis, D., Thrassou, A. and Ghosh, S.K. (2021), "ICT-enabled CRM system adoption: a dual Indian qualitative case study and conceptual framework development", *Journal of Asia Business Studies*, Vol. 15 No. 2, pp. 257-277, doi: 10.1108JABS-05-2020-0198.

Chen, Q., Min, C., Zhang, W., Wang, G., Ma, X. and Evans, R. (2020), "Unpacking the black box: howto promote citizen engagement through government social media during the COVID-19 crisis", *Computers in Human Behavior, Vo\.* 110, p. 106380, doi: 10.1016/j.chb.2020.106380.

Cheng, J.W., Mitomo, H., Otsuka, T. and Jeon, S.Y. (2016), "Cultivation effects of mass and social media on perceptions and behavioural intentions in post-disaster recovery: the case of the 2011 great east Japan earthquake", *Telematics and Informatics*, Vol. 33 No. 3, pp. 753-772, doi: 10.1016/ J.TELE.2015.12.001.

Chin, W. (1998a), "Issues and opinion on structural equation modeling", *Mis Q*, Vol. 22 No. 1, pp. 7-16.

Chin, W.W. (1998b), "The partial least squares approach to structural equation modeling", *Modern Methods for Business Research, Mahwah, NJ*, Vol. 295 No. 2, pp. 295-336.

Cohen, J. (1988), *In Statistical Power Analysis for the Behavioral Sciences*, (2nd Ed.), Lawrence Erlbaum Associates, Hillsdale, NJ.

Collier, J.E. and Sherrell, D.L. (2009), "Examining the influence of control and convenience in a self-service setting", *Journal of the Academy of Marketing Science*, Vol. 38 No. 4, pp. 490-509, doi: 10.1007/ S11747-009-0179-4/METRICS.

Criado, J.I., Sandoval-Almazan, R. and Gil-Garcia, J.R. (2013), "Government innovation through social media", *Government Information Quarterly*, Vol. 30 No. 4, pp. 319-326, doi: 10.1016/J.GIQ.2013.10.003.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R. (2013), "Future directions for behavioral information security research", *Computers & Security*, Vol. 32, pp. 90-101, doi: 10.1016/J.C0SE.2012.09.010.

Farooq, A., Laato, S. and Najmul Islam, A.K.M. (2020), "Impact of online information on self-isolation intention during the COVID-19 pandemic: cross-sectional study", *Journal of Medical Internet Research*, Vol. 22 No. 5, p. e19128, doi: 10.2196/19128.

Floyd, D.L., Prentice-Dunn, S. and Rogers, R.W. (2006), "A meta-analysis of research on protection motivation theory", *Journal of Applied Social Psychology*, Vol. 30 No. 2, pp. 407-429, doi: 10.1111/ J. 1559-1816.2000.TB02323.X.

Fornell, C. and Larcker, D.F. (1981), "Evaluating structural equation models with unobservable variables and measurement error", *Journal of Marketing Research*, Vol. 18 No. 1, pp. 39-50.

Gefen, D., Straub, D. and Boudreau, M.-C. (2000), "Structural equation modeling and regression: guidelines for research practice", *Communications of the Association for Information Systems*, Vol. 4 No. 1, p. 7.

Gerbner, G. and Gross, L. (1976), "Living with television: the violence profile", *Journal of Communication*, Vol. 26 No. 2, pp. 172-199, doi: 10.1111/J.1460-2466.1976.TB01397.X.

Gerbner, G., Gross, L., Morgan, M., Shanahan, J. and Signorielli, N. (2009), "Growing up with television: cultivation processes", (2nd Ed.), *Media Effects*, Advances in Theory and Research, Routledge, New York, NY, pp. 34-49, doi: 10.4324/9781410602428-7.

Guo, J., Liu, N., Wu, Y. and Zhang, C. (2021), "Why do citizens participate on government social media accounts during crises? A civic voluntarism perspective", *Information & Management*, Vol. 58 No. 1, doi: 10.1016/j.im.2020.103286.

Hair, J.F. (2011), "Multivariate data analysis: an overview", in Lovric, M. (Ed.), *International Encyclopedia of Statistical Science*, Springer, Berlin, pp. 904-907, doi: 10.1007/978-3-642-04898-2_395.

Hair, J.F., Jr., Hult, G.T.M., Ringle, C.M. and Sarstedt, M. (2014), "A primer on partial least squares structural equations modeling (PLS-SEM)", *European Journal of Tourism Research*, Vol. 6 No. 2, pp. 211-213.

Han, J.Y., Kim, Y.J. and Kim, H. (2017), "An integrative model of information security policy compliance with psychological contract: examining a bilateral perspective", *Computers & Security*, Vol. 66, pp. 52-65, doi: 10.1016/j.cose.2016.12.016.

Hanus, B. and Wu, Y. (2016), "Impact of users' security awareness on desktop security behavior: a protection motivation theory perspective", *Information Systems Management*, Vol. 33 No. 1, pp. 2-16, doi: 10.1080/10580530.2015.1117842.

Harris, M.A. and Patten, K.P. (2014), "Mobile device security considerations for small- and medium-sized enterprise business mobility", *Information Management and Computer Security*, Vol. 22 No. 1, pp. 97-114, doi: 10.1108/IMCS-03-2013-0019/FULL/XML.

He, W. (2012), "A review of social media security risks and mitigation techniques", *Journal of Systems and Information Technology, Vol.* 14 No. 2, pp.171-180, doi: 10.1108/13287261211232180.

He, W. (2013), "A survey of security risks of mobile social media through blog mining and an extensive literature search", *Information Management & Computer Security*, Vol. 21 No. 5, pp. 381-400, doi: 10.1108/IMCS-12-2012-0068.

Hermann, E., Eisend, M. and Bayon, T. (2020), "Facebook and the cultivation of ethnic diversity perceptions and attitudes", Internet Research, Vol. 30 No. 4, pp. 1123-1141, doi: 10.1108/INTR-10-2019-0423/FULL/XML.

Hina, S., Panneer Selvam, D.D.D. and Lowry, P.B. (2019), "Institutional governance and protection motivation: theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world", *Computers & Security*, Vol. 87, p. 101594, doi: 10.1016/j.cose.2019.101594.

Hooper, V. and Blunt, C. (2020), "Factors influencing the information security behaviour of IT employees", *Behaviour & Information Technology*, Vol. 39 No. 8, pp. 862-874, doi: 10.1080/0144929X.2019.1623322.

Ifinedo, P. (2012), "Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory", *Computers & Security*, Vol. 31 No. 1, pp. 83-95, doi: 10.1016/j.cose.2011.10.007.

Intravia, J., Wolff, K.T., Paez, R. and Gibbs, B.R. (2017), "Investigating the relationship between social media consumption and fear of crime: a partial analysis of mostly young adults", *Computers in Human Behavior,Vol.77*, pp. 158-168, doi: 10.1016/J.CHB.2017.08.047.

Johnson, R.D. and Marakas, G.M. (2000), "The role of behavioral modeling in computer skills acquisition: toward refinement of the model", *Information Systems Research, INFORMS*, Vol. 11 No. 4, pp. 402-417, doi: 10.1287/ISRE.11.4.402.11869.

Johnston, A.C. and Warkentin, M. (2010), "Fear appeals and information security behaviors: an empirical study", *MIS Quarterly: Management Information Systems*, Vol. 34 No. 3, pp. 549-566, doi: 10.2307/25750691.

Johnston, A.C., Warkentin, M., Dennis, A.R. and Siponen, M. (2019), "Speak their language: designing effective messages to improve employees' information security decision making", *Decision Sciences*, Vol. 50 No. 2, pp. 245-284, doi: 10.1111/DECI.12328.

Kannan, V.R. and Tan, K.C. (2005), "Just in time, total quality management, and supply chain management: understanding their linkages and impacton business performance", *Omega*, Vol. 33 No. 2, pp. 153-162, doi: 10.1016/j.omega.2004.03.012.

Kim, S.C. and Hawkins, K.H. (2020), "The psychology of social media communication in influencing prevention intentions during the 2019 U.S. measles outbreak", *Computers in Human Behavior*, Vol. 111, p. 106428, doi: 10.1016/J.CHB.2020.106428.

Kock, N. (2015), "Common method bias in PLS-SEM: a full collinearity assessment approach", *International Journal of e-Collaboration*, Vol. 11 No. 4, pp. 1-10.

Lebek, B., Uffen, J., Neumann, M., Hohler, B.H. and Breitner, M. (2014), "Information security awareness and behavior: a theory-based literature review", *Management Research Review*, Vol. 37 No. 12, pp. 1049-1092, doi: 10.1108/MRR-04-2013-0085.

Lee, M.J. and Cho, H. (2018), "Uses of social media in government agencies: content analyses of public relations strategies and message tactics comparison between South Korea and the United States of America in 2011 and 2014", *Journal of Public Affairs*, Vol. 18 No. 2, p. e1687, doi: 10.1002/PA.1687.

Liang, H. and Xue, Y. (2010), "Understanding security behaviors in personal computer usage: a threat avoidance perspective", *Journal of the Association for Information Systems*, Vol. 11 No. 7, p. 1, doi: 10.17705/1jais.00232.

Li, Y., Chandra, Y. and Fan, Y. (2022), "Unpacking government social media messaging strategies during the COVID-19 pandemic in China", *Policy & Internet*, Vol. 14 No. 3, pp. 651-672, doi: 10.1002/ POI3.282.

Li, L., He, W., Xu, L., Ash, I., Anwar, M. and Yuan, X. (2019), "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior", *International Journal of Information Management*, Vol. 45, pp. 13-24, doi: 10.1016/j.ijinfomgt.2018.10.017.

Ma, X. (2022), "Is professionals' information security behaviors in Chinese IT organizations for information security protection", *Information Processing & Management*, Vol. 59 No. 1, p. 102744, doi: 10.1016/j. ipm.2021.102744.

Maddux, J.E. and Rogers, R.W. (1983), "Protection motivation and self-efficacy: a revised theory of fear appeals and attitude change", *Journal of Experimental Social Psychology*, Vol. 19 No. 5, pp. 469-479, doi: 10.1016/0022-1031(83)90023-9.

Martens, M., De Wolf, R. and De Marez, L. (2019), "Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general", *Computers in Human Behavior*, Vol. 92, pp. 139-150, doi: 10.1016/J.CHB.2018.11.002.

Medaglia, R. and Zhu, D. (2017), "Public deliberation on government-managed social media: a study on Weibo users in China", *Government Information Quarterly,* Vol. 34 No. 3, pp. 533-544, doi: 10.1016/j. giq.2017.05.003.

Moody, G.D., Siponen, M. and Pahnila, S. (2018), "Toward a unified model of information security policy compliance", *MIS Quarterly,* Vol. 42 No. 1, pp. 285-311, doi: 10.25300/MISQ/2018/13853.

Nair, J., Chellasamy, A. and Singh, B.N.B. (2019), "Readiness factors for information technology adoption in SMEs: testing an exploratory model in an Indian context", *Journal of Asia Business Studies,* Vol. 13 No. 4, pp. 694-718, doi: 10.1108/JABS-09-2018-0254.

Nguyen, T.T.U., Nguyen, P., Van, Huynh, H.T.N., Vrontis, D. and Ahmed, Z.U. (2023), "Identification of the determinants of public trust in e-government services and participation in social media based on good governance theory and the technology acceptance model", *Journal of Asia Business Studies,* doi: 10.1108/JABS-04-2023-0160.

Perez-Moron, J. (2022), "Eleven years of cyberattacks on Chinese supply chains in an era of cyber warfare, a review and future research agenda", *Journal of Asia Business Studies,* Vol. 16 No. 2, pp. 371-395, doi: 10.1108/JABS-11-2020-0444.

Posey, C., Roberts, T.L. and Lowry, P.B. (2015), "The impact of organizational commitment on insiders motivation to protect organizational information assets", *Journal of Management Information Systems*, Vol. 32 No. 4, pp. 179-214, doi: 10.1080/07421222.2015.1138374.

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A. and Herawan, T. (2015), "Information security conscious care behaviour formation in organizations", *Computers & Security,* Vol. 53, pp. 65-78, doi: 10.1016/j.cose.2015.05.012.

Shah, Z., Chu, J., Ghani, U., Qaisar, S. and Hassan, Z. (2020), "Media and altruistic behaviors: the mediating role of fear of victimization in cultivation theory perspective", *International Journal of Disaster Risk Reduction,* Vol. 42, p. 101336,doi: 10.1016/J.IJDRR.2019.101336.

Sharma, S., Singh, G., Sharma, R., Jones, P., Kraus, S. and Dwivedi, Y.K. (2020), "Digital health innovation: exploring adoption of COVID-19 digital contact tracing apps", *IEEE Transactions on Engineering Management,* doi: 10.1109/TEM.2020.3019033.

Siponen, M. and Vance, A. (2010), "Neutralization: new insights into the problem of employee information systems security policy violations", *MIS Quarterly: Management Information Systems,* Vol. 34 No. 3, pp. 487-502, doi: 10.2307/25750688.

Siponen, M., Adam Mahmood, M. and Pahnila, S. (2014), "Employees' adherence to information security policies: an exploratory field study", *Information & Management,* Vol. 51 No. 2, pp. 217-224, doi: 10.1016/ j.im.2013.08.006.

Tang, Z., Miller, A.S., Zhou, Z. and Warkentin, M. (2021), "Does government social media promote users' information security behavior towards COVID-19 scams? Cultivation effects and protective motivations", *Government Information Quarterly,* Vol. 38 No. 2, p. 101572, doi: 10.1016/j.giq.2021.101572.

Tu, Z., Turel, O., Yuan, Y. and Archer, N. (2015), "Learning to cope with information security risks regarding mobile device loss or theft: an empirical examination", *Information & Management,* Vol. 52 No. 4, pp. 506-517, doi: 10.1016/J.IM.2015.03.002.

Wall, J.D. and Warkentin, M. (2019), "Perceived argument quality's effect on threat and coping appraisals in fear appeals: an experiment and exploration of realism check heuristics", *Information & Management,* Vol. 56 No. 8, p. 103157, doi: 10.1016/J.IM.2019.03.002.

Warkentin, M., Johnston, A.C. and Shropshire, J. (2011), "The influence of the informal social learning environment on information privacy policy compliance efficacy and intention", *European Journal of Information Systems,* Vol. 20 No. 3, pp. 267-284, doi: 10.1057/EJIS.2010.72.

Warkentin, M., Johnston, A.C., Shropshire, J. and Barnett, W.D. (2016), "Continuance of protective security behavior: a longitudinal study", *Decision Support Systems,* Vol. 92, pp. 25-35, doi: 10.1016/J. DSS.2016.09.013.

Witte, K., Cameron, K.A., McKeon, J.K. and Berkowitz, J.M. (2010), "Predicting risk behaviors: development and validation of a diagnostic scale", *Journal of Health Communication,* Vol. 1 No. 4, pp. 317-341, doi: 10.1080/108107396127988.

Wong, L.W., Lee, V.H., Tan, G.W.H., Ooi, K.B. and Sohal, A. (2022), "The role of cybersecurity and policy awareness in shifting employee compliance attitudes: building supply chain capabilities", *International Journal of Information Management,* Vol. 66, p. 102520, doi: 10.1016/j.ijinfomgt.2022.102520.

Wu, D. (2020), "Empirical study of knowledge withholding in cyberspace: integrating protection motivation theory and theory of reasoned behavior", *Computers in Human Behavior,* Vol. 105, p. 106229, doi: 10.1016/J.CHB.2019.106229.

Yin, F., Xia, X., Pan, Y., She, Y., Feng, X. and Wu, J. (2022), "Sentiment mutation and negative emotion contagion dynamics in social media: a case study on the Chinese sina microblog", *Information Sciences*, Vol. 594, pp. 118-135, doi: 10.1016/J.INS.2022.02.029.

Zhang, X.J., Li, Z. and Deng, H. (2017), "Information security behaviors of smartphone users in China: an empirical analysis", *The Electronic Library*, Vol. 35 No. 6, pp. 1177-1190, doi: 10.1108/EL-09-2016-0183/ FULL/XML.

Appendix

Table A1

Constructs	*Item no.*	*Measurement*	*Adapted sources*	*Changes*
Government social media (GSM)	GSM1	I always read and listen to cybersecurity warnings posted by GSM	Tang *etal.* (2021)	Minor change
	GSM2	I always share the cybersecurity warnings posted by GSM		Minor change
	GSM3	I always recommend to others the cybersecurity warnings posted by government agencies on social media		Minor change
Perceived threat vulnerability (PV)	PV1	I am aware that if I do not adhere to my institution's information security policies, my institution may be susceptible to security breaches	Hina *etal.* (2019), Li *etal.* (2019); and Wong *et al.* (2022)	Major change
	PV2	If I do not adhere to my institution's information security policies, I may become a victim of a malicious attack		Major change
	PV3	My computing resources at my workplace can be susceptible to information security threats		Major change
	PV4	I believe that my efforts to protect the information of my organization will reduce unauthorized access to it		Major change
	PV5	Companies should be encouraged to use up-to-date cybersecurity technologies		Major change
	PV6	The staff must be regularly briefed on potential threats		Major change
	PV7	It is probable that the potential information security breach will affect the information and information systems of my organization		Major change
Self-efficacy (SE)	SE1	I am confident in my ability to defend myself against information security breaches	Hina *etal.* (2019), Li *etal.* (2019); and Wong *et al.* (2022)	Minor change
	SE2	I believe I have developed the ability to prevent unauthorized access to my private information		Minor change
	SE3	On my computing resources at work, I take security measures (firewall and antivirus)		Self-development
	SE4	I believe that protecting myself from information security breaches is within my control		Minor change
	SE5	I am confident about adjusting the website browser's security settings to various levels		Self-development
	SE6	I am comfortable working with virus-infected files		Self-development
	SE7	I am confident in my ability to eliminate spyware and malware from my computer		Minor change
Response efficacy (RE)	RE1	My institution's efforts to protect the confidentiality of my sensitive information are effective	Hina *etal.* (2019), Li *etal.* (2019); and Wong *et al.* (2022)	Major change
	RE2	Effective security measures exist at my institution to protect my work information from security breaches		Major change
	RE3	Effective preventative measures exist at my institution for dealing with malicious content		Major change
	RE4	My institution's security measures effectively prevent hackers from gaining access to sensitive personal or academic data		Major change

	RE5	Compliance with my organization's information security policies will reduce security breaches		Minor change
	RE6	Following information security policies can lead to a reduction in the frequency of information security breaches		Minor change
	RE7	Adhering to information security policies helps in preventing security issues		Minor change
	RE8	Demonstrating to employees how their security negligence impacts the security posture of an organization can lead to an improvement in their security behavior		Major change
	RE9	The information security policies at my institution are effective in reducing information security incidents		Minor change

(continued)

Table A1

Constructs	*Item no.*	*Measurement*	*Adapted sources*	*Changes*
	RE10	Upgrading of antivirus and firewall software at my organization helps in preventing security risks		Minor change
Cybersecurity compliance attitude (ATT)	ATT1	I believe that my institution's information security policies must be followed without exception	Hina *etal.* (2019)	Minor change
	ATT2	I find it reasonable to comply with information security policies		Minor change
	ATT3	I strongly believe that complying with my institution's information security policies is an excellent idea		Minor change
Information protection motivation (IPM)	IPM1	I am committed to protecting my organization from information security risks	Ma (2022) and Posey *et al.* (2015)	Minor change
	IPM2	My intention to thwart the success of information security threats to my organization is strong		Minor change
	IPM3	I am likely to take action to safeguard the information and information systems of my organization against security threats		Major change
	IPM4	I am committed to making an effort to protect my organization from information security risks		Major change
	IPM5	I am determined to take all necessary measures to prevent information security threats from occurring at my organization		Major change
Employee protective behaviors (EPB)	EPB1	I maintain current antivirus software on my computer	Li *etal.* (2019)	Minor change
	EPB2	I keep an eye out for odd computer behavior and responses		Minor change
	EPB3	I always respond to any malware warnings that I receive		Minor change

Source: Created by the authors

From awareness to behaviour: From awareness to understanding cybersecurity compliance in Vietnam

Dien Van Tran, Phuong V. Nguyen and Linh Phuong Le, Sam Thi Ngoc Nguyen.

Center for Public Administration, International University, Vietnam National University - HCMC, Ho Chi Minh City, Vietnam, and School of Business, International

University, Vietnam National University-HCMC,
Ho Chi Minh City, Vietnam

Abstract
Purpose - This paper aims to investigate the in**fl**uence of cybersecurity awareness and compliance attitudes on the protective behaviours exhibited by employees. This study also aims to explore the complex correlation between the level of awareness about cybersecurity measures and attitudes towards compliance with these measures. Additionally, it looks at how these factors collectively impact employees' behaviour to protect organisational assets and information.
Design/methodology/approach - This study uses a quantitative research methodology in which primary data are gathered using a survey questionnaire distributed to personnel employed at Vietnamese organisations. The data are analysed, and the validity of the measurement and structural equation model is assessed using a partial least squares-structural equation model approach after the collection of all the survey responses.
Findings - The provision of policies and security education, training and awareness programmes are strongly and positively associated with cybersecurity awareness. Moreover, cybersecurity awareness plays an important role in shaping attitudes and intentions towards information security policy compliance (ISPC). Attitude is positively associated with intention towards ISPC and employee protective behaviour. Finally, the intention towards ISPC is signi**fi**cant in shaping employee protective behaviour.
Originality/value - This study contributes to the understanding of the antecedents of cybersecurity in developing countries such as Vietnam. Furthermore, it provides a comprehensive framework for understanding intention and protective behaviour through cybersecurity awareness and compliance attitudes. By combining the theory of planned behaviour and protection motivation theory with institutional governance, this study extends previous research on the effects of these variables on employee protective behaviour.

Keywords Cybersecurity awareness, Cybersecurity compliance attitude, Institutional governance, Protective behaviour
Paper type Research paper

1. Introduction

Information and communication technology is undergoing a dramatic shift, and the rise of the Internet of Things has led to a revolution in cyber-physical systems and provided users with a wealth of new benefits, especially in Vietnam. The internet has opened up new economic opportunities for individuals and businesses alike by streamlining the process of conducting transactions via mobile devices and facilitating connections with new people through social networks (Lee *et al.*, 2017; Saadatdoost *et al.*, 2015). Sustainable development goals are often considered a way in which to enable developing countries to catch up quickly

 with developed countries (Michael *et al.*, 2019). Because of the vital role that it plays in the economy and society at large, several governments have deemed the internet part of their country's critical infrastructure (Chang and Coppel, 2020). Although its rapid expansion opens promising new avenues for progress, it also poses some concerning risks (Ani *et al.*, 2017). Furthermore, in the realm of security, threats are typically directed at organisational assets rather than personal assets (Menard et al., 2017). The cost of managing cyber risks in the event of an attack could be substantial in the absence of adequate risk reduction, incident handling strategies and effective cybersecurity awareness campaigns (Wong et al., 2022). As a result, studies on the best practices for establishing and maintaining secure cyber capabilities at organisations are urgently needed in less developed countries.
To ensure that businesses can continue to function securely and efficiently in the digital age, it is important to ensure that employees are motivated to act in a way that is compatible with information security policies. Because of the diversity of personnel, management, partners and infrastructure at every organisation, internal vulnerabilities are difficult to control (Roy Sarkar, 2010). Internal security breaches, whether deliberate or accidental, are more difficult to detect and investigate than any other threats (Barlow et al., 2013). That is why it is crucial to look at what makes people comply with information security systems and protect them. Therefore, if employees are not adequately educated on the topic of cybersecurity, the company will be vulnerable to the severe threats present in their external business environment. Their lack of awareness could indicate negative or resistant behaviour, which has the potential to compromise the safety of the business and its data (Bulgurcu *etal.*, 2010; Donalds and Osei-Bryson, 2020; Hu *etal.*, 2007). In addition, a positive outlook towards following the policies that govern the security of information systems is a strong indicator that the employee will follow them (Ifinedo, 2012; Venkatesh et al., 2003).
Because of the growing availability of internet connectivity, the level of sophistication and frequency of cyberattacks have noticeably risen. The continuation of this detrimental behaviour has had significant and extensive negative consequences, affecting not only businesses and entire sectors but also national governments (Tran et al., 2024). Consequently, governments have enacted targeted measures to protect networks associated with national security. The goal is to enhance the legal structure of network information security to guarantee the strong safeguarding of vital national defence information. To achieve this, governments must prioritise an evaluation of the capabilities and practical expertise of the people in charge of the networks. Moreover, the establishment of a comprehensive legislative framework is essential for effective control of network information

security, especially to mitigate risks and counteract threats in the digital realm. The Vietnamese Congress passed the Cybersecurity Law on 12 June 2018, and it became effective on 1 January 2019. The objective of this law is to oversee actions intended to maintain social order and security in the digital domain, specifying the responsibilities of pertinent authorities, organisations and individuals. However, it is essential to conduct further research and enhance institutional governance in terms of security, education, training and awareness (SETA) programmes and the provision of policies. This is imperative to ensure the safety of employees in the workplace during internet usage and online transactions.

Intentional behaviour is intricately tied to both cybersecurity awareness and attitude (Sommestad et al., 2015; Wiafe et al., 2020), but just a few comprehensive studies of awareness, attitude, intention and behaviour have combined theories of planned behaviour (TPB) and protection motivation theory (PMT) with institutional governance (IG). IG is demonstrated to be strongly motivated by employee protection behaviour in policy compliance (Hina et al., 2019). However, little is understood about how these factors influence employees' awareness, leaving a gap in the literature that our research fills by

exploring the factors that may inspire employees to comply with security policies and by encouraging the discovery and improvement of awareness of antecedents' attitudes. Hence, in this study, we integrate TPB and PMT into a research framework to investigate the interplay between employee cybersecurity awareness and attitude towards compliance as an explicit measure of employee protective behaviour under institutional governance. Specifically, we address the following research questions:

RQ1. How does institutional governance influence cybersecurity awareness?

RQ2. What is the impact of cybersecurity awareness on the relationship between employee protective behaviour and a cybersecurity compliance attitude with a mediating role played by intention towards information security policy compliance (ISPC)?

The rest of this paper proceeds as follows: Section 2 reviews the literature and formulates our hypotheses. Section 3 describes the data and the research model. Section 4 provides empirical results. Section 5 discusses the findings. Section 6 describes the theoretical and practical contributions. Section 7 concludes the paper, describes the limitations and offers some recommendations for further research.

2. Literature review and hypothesis development

2.1 Protection motivation theory

The PMT was first introduced by Rogers (1975) to depict the incentives of people to engage in protective behaviours when they are exposed to a danger signal. It also implies that people are motivated to engage in risk-avoidant activity because they want to keep themselves safe (Janmaimool, 2017). Specifically, this theory posits that when individuals are faced with the potential for a negative outcome, they typically adopt a certain set of cognitive processes to decide how to react. Moreover, it is structured in terms of two processes: threat appraisal and coping appraisal.
First, threat appraisal is a cognitive process that people use to evaluate risk. It takes into account three important elements considered antecedents of individuals' adaptive actions: threat vulnerability, threat severity and threat susceptibility (Rippetoe and Rogers, 1987). Second, coping appraisal is described as an individual's capacity to engage in protective behaviours when facing a threat (Janmaimool, 2017). Importantly, the elements of the coping appraisal are response efficacy, self-efficacy and response cost (Li *et al.*, 2019).
PMT has been validated in psychology (Floyd *et al.*, 2000), research conducted on information security (Vance *et al.*, 2012; Wall and Warkentin, 2019), home computer use (Tsai *et al.*, 2016), consumers (Kim *et al.*, 2022) and anti-plagiarism software adoption (Lee, 2011). Thus, PMT provides a solid framework for building a research model to incorporate cybersecurity awareness into this study.

2.2 Theory of planned behaviour

The TPB is a behaviour model commonly used to explain and indicate the role of an intrinsic driver in shaping human behaviour. Moreover, this theory holds that people are rational and have beliefs and knowledge, which are obtained systematically through personal experiences, formal education, media and interactions with family and friends. As a result, they tend to interpret and remember to determine their deliberate conduct. Individual attitudes and subjective norms about performing a behaviour shape a behavioural intention, which is an essential element of actual behaviour (Ajzen, 1991). Specifically, the TPB has been adopted in e-service (Liao *et al.*, 2007), communication technologies (Moletsane and Tsibolane, 2020; Teo and Beng Lee, 2010; Yousuf *et al.*, 2023),

 health communication (Wu and Kuang, 2021) and information security (Alanazi *et al.*, 2022).
This study expands upon the TPB's examination of the impact of attitude and intention on employee behaviour.

2.3 Cybersecurity awareness

The importance of security awareness in perceiving dangers that threaten workplace resources needs to be emphasised (Bulgurcu *et al.*, 2010). In addition, information security awareness refers to the extent to which users comprehend the significance of information security and their obligations and actions in performing aspects of information security control adequately to secure the firm's data and networks (Shaw *et al.*, 2009). Similarly, cybersecurity awareness refers to the knowledge and practice of securing a firm's digital infrastructure (Alghamdi, 2021).

Self-efficacy, response efficacy and perceived barriers are all regarded as crucial factors in determining the level of cybersecurity awareness (Alghamdi, 2021). The PMT serves as the foundation for the development of this construct, which is shown to be a second-order construct. This construct consists of self-efficacy, response efficacy and perceived barriers, thereby measuring specific aspects of cybersecurity awareness. This second-order construct enables the incorporation of three different aspects of cybersecurity awareness. It provides a comprehensive and holistic representation of the concept, capturing its multifaceted nature.

First, self-efficacy is the assessment of a person's capacity for protective behaviour - whether the individual has the skills, experience and tools required to perform work responsibly (Maddux and Rogers, 1983). Similarly, when people believe in their own skills as well as having a high level of self-efficacy to accomplish a goal, they are more likely to take the next step towards realising that goal. Second, response efficacy evaluates the effectiveness of an adaptive reaction to mitigate a threat (Rogers, 1975). Likewise, response efficacy refers to employees' confidence that a suggested action would successfully mitigate an existing hazard (Boss *et al.*, 2015). Finally, perceived barriers refer to the employee's perceived inconvenience and expense associated with engaging in cybersecurity protection activities (Li *etal.*, 2019).

2.4 Institutional governance and cybersecurity awareness

Institutional governance includes the establishment of policies, responsibilities, standards and guidelines to ensure the secure and appropriate use of information system resources (D'Arcy *et al.*, 2009). More precisely, this study focuses on the concentration of institutional governance in the areas of the provision of policies as well as SETA programmes.

First, because of its comprehensive outline of employee responsibilities and the consequences of non-compliance, a security policy is very likely to capture the attention of employees and enhance their understanding of security measures (Hwang *et al.*, 2021). Likewise, employees may encounter difficulties in comprehending and implementing policies if they are excessively complex. Moreover, they may encounter confusion or a lack of confidence because of uncertainty over the appropriate course of action. Thus, the visibility of policies greatly influences the degree to which employees adhere to them in relation to organisational security (Siponen *et al.*, 2009). Furthermore, a lack of security standards may contribute to confusion about the definition of effective system functionality (Straub, 1990). Corporate information security policies are a fundamental component of strategies for managing information system security (Chan *et al.*, 2005). Importantly, prior empirical studies have demonstrated a strong relationship between the provision of policies and security awareness (Chan *etal.*, 2005; Hwang *et al.*, 2021; Zwilling *etal.*, 2022).

Second, SETA programmes serve as the primary means of spreading protection-
From

motivated behaviours at firms and, therefore, are valuable precursors to PMT assessment awareness to (Posey *et al.*, 2015).
In particular, SETA programmes use various formats, such as seminars,
behaviour

workshops and drills, to emphasise and enhance employees' security knowledge, awareness and capabilities. The events aim to educate employees about the company's information security architecture, as well as its policies, procedures and practices, to ensure regulatory compliance. These programmes are designed to equip employees with the necessary information and expertise to identify risks, implement preventive actions, comply with rules

---

and procedures and maintain security (Lee and Lee, 2002; Whitman, 2003). Similarly, effectively implemented SETA programmes can educate employees on the hazards that they encounter, the gravity of security risks that they face and the optimal methods for safeguarding themselves against such risks (Zwilling et al., 2022), thereby facilitating widespread awareness of the significance of an information system policy (Chen et al., 2015). Essentially, security education has been demonstrated to enhance employees' understanding of and interest in the matter (Siponen et al., 2009), ultimately decreasing risky behaviour (Eminagaoglu *etal.*, 2009). Furthermore, it is evident that education and training can raise the competence of personnel to perform their duties (Chen et al., 2015).

Understanding information security is essential for preventing data breaches in the presence of increasing risks and vulnerabilities (Allam et al., 2014). Scholars also highlight the impact of SETA programmes on employees' cybersecurity awareness (D'Arcy et al., 2009; McCrohan et al., 2010; Posey et al., 2015; Siponen et al., 2009). Specifically, SETA

programmes are proven to have a positive connection with self-efficacy (Hina et al., 2019) and response efficacy (Workman, 2009). In general, training programmes raise participants' level of knowledge about security and improve their propensity to act safely in the workplace. Because SETA promotes the merits of established safety procedures, this study examines the notion that individuals who adhere to institutional governance in terms of the provision of policies and SETA programmes are more likely to have a heightened level of cybersecurity awareness. Therefore, we propose the following hypotheses:

. The provision of policies is positively related to cybersecurity awareness.

H2. SETA programmes are positively related to cybersecurity awareness.

2.5 Cyóersecnrity awareness and intention towards information secnrity policy compliance Integration of the PMT's core elements - self-efficacy, response efficacy and perceived barriers - enables a more comprehensive evaluation of cybersecurity awareness. When employees understand the seriousness of the security threats that their firm encounters, they are more motivated to follow established information security measures (Siponen et al., 2009). Employees' failure to implement basic security measures is caused by information security hurdles (Ng et al., 2009). When employees believe that the barriers to enforcing cybersecurity regulations are strong, they are less inclined to adopt precautionary measures. Furthermore, employees are highly motivated to follow these regulations because of their high levels of self-efficacy and response efficacy (Siponen et al., 2009). The PMT indicates that sensitivity may temper protective responses, such as going the extra mile to ensure one's own safety (Herath and Rao, 2009; Ifinedo, 2012; Vance et al., 2012).

Senior management and information technology security staff must prioritise information security in any organisation (Safa et al., 2016). Information security includes technical and non-technical measures. Technical measures of information security at organisations include hardware measures such as firewalls, antivirus software, data

 backup, access control, encryption and continuous monitoring to detect threats (Ifinedo, 2012). Meanwhile, non-technical measures include human and organisational behaviour (Ifinedo, 2014). These measures improve ISPC by applying sociological, psychological and organisational behaviour theories to information security (Ifinedo, 2014).

In particular, previous empirical studies illustrate that perceived awareness of cyber threats strongly influences cybersecurity behaviours (Alanazi *et al.*, 2022; Dinev and Hu, 2007; Meso et al., 2013). Instructions on how to avoid harm raise people's awareness of possible threats (van Bavel et al., 2019). Therefore, we propose a new hypothesis that delves more deeply into the effect of ISPC on increasing individual awareness and, consequently, improving cybersecurity behaviours:

H3. Cybersecurity awareness is positively related to an intention towards ISPC.

2.6 Cybersecurity awareness and a compliance attitude

Ensuring information security depends greatly on fostering awareness. Specifically, our attitudes play a pivotal role in influencing the stimuli on which we choose to focus and that we choose to ignore, functioning as essential factors that shape human behaviour. People's "attitudes" refer to their emotional response to a particular act, reflecting a trained tendency to evaluate things in a given manner. Attitudes are moulded by people's viewpoints, intentions and knowledge, which collectively influence their outlook on a particular object. Individuals who have a positive disposition towards a specific matter are more inclined to demonstrate the constructive behaviours associated with it. Furthermore, when individuals consider a particular threat to be substantial, they recognise the need for compliance attitudes that minimise risk. But if they do not regard the threat as relevant, their recognition of its importance is lower (Hina *et al.*, 2019; Menard *et al.*, 2017). Similarly, individuals who believe that they are impervious to risk are less likely to engage in precautionary measures to mitigate it. Consequently, their chances of sustaining injuries are higher (Ifinedo, 2012). Essentially, policies are better understood after awareness-raising campaigns, and, consequently, people generally have a more positive outlook on complying with them (Dinev and Hu, 2007; Ma, 2022; Parsons *et al.*, 2014; Williams, 2008). Hence, we speculate that an employee with a heightened perception of vulnerability demonstrates more compliance with security awareness policies and makes additional effort to maintain the integrity of task security. Thus, the following hypothesis is proposed:

H4. Cybersecurity awareness is positively related to compliance attitude.

2.7 Cybersecurity compliance attitude, information security policy compliance and employee protective behaviour

According to TPB, people's attitudes are the driving force behind their actions (Ajzen, 1991). Given that attitude is a strong predictor of intention, it is crucial to perform TPB studies on this aspect (Bulgurcu *et al.*, 2010; Ifinedo, 2012; Mahon *et al.*, 2006; Zhang *et al.*, 2009). Individuals are more likely to comply with laws and regulations if they have a positive attitude

towards doing so. Hence, a positive disposition towards ISPC implies a willingness to engage in activities that maintain ISPC. Likewise, strong attitudes, marked by high levels of confidence and consistency, are more likely to affect behaviour. A positive opinion of ISPC greatly increases the probability of compliance with regulations (Wiafe *et al.*, 2020).

Empirical research has shown that holding a positive attitude towards cybersecurity regulations results in a higher level of compliance with norms and standards related to ISPC

(Bulgurcu *et al.*, 2010; Dinev and Hu, 2007; Guo *et al.*, 2011; Herath and Rao, 2009; Ng *et al.*, 2009; Siponen et al., 2014; Swaim et al., 2014). This, in turn, has a substantial impact on employees' adoption of protective behaviours (Maalem Lahcen et al., 2020; Ng et al., 2009; Siponen et al., 2014). Therefore, we assume that individuals with a cybersecurity compliance attitude have a positive attitude towards engaging in ISPC and protective behaviour. Based on these arguments, the fifth and sixth hypotheses are proposed:

H5. Cybersecurity compliance attitude is positively related to intention towards ISPC.

H6. Cybersecurity compliance attitude is positively related to employee protective behaviour.

2.8 Intention towards information security policy compliance, cybersecurity awareness and employee protective behaviour

First, intention is a crucial factor in anticipating behaviour because it reveals a motivation for engaging in that behaviour (Armitage and Conner, 2001). According to the TPB, an individual's intention is a cognitive representation of the purpose that precedes action and is therefore the direct antecedent of the behaviour (Ajzen, 1985). In other words, the possibility that people engage in a desirable behaviour will be borne out depends on the interest in that behaviour that they feel. Similarly, it is assumed that individuals take actions consistent with their goals when presented with an attractive opportunity and they evaluate them as beneficial incentives. It has been well established that intention towards ISPC plays a part in determining employees' protective behaviour (Swaim *et al.*, 2014).

Second, employees need to be informed of the risks in the cyber world so that they can take measures to protect themselves and their firm. Employees are less likely to implement cybersecurity procedures enthusiastically if they perceive substantial barriers (Ng and Xu, 2007). They become more cautious about potentially risky behaviours that could jeopardise corporate security. Moreover, they are more inclined to take safety precautions if they believe they have the skills to respond successfully to any given scenario (Johnston and Warkentin, 2010). A high sense of self-efficacy in cybersecurity means that employees are confident about their ability to implement additional security measures. In other words, they are more inclined to practice safety awareness and preventive measures. Therefore, employees are more likely to abide by information security policies if they are made aware of the likelihood and consequences of disobeying those policies (Tsohou *et al.*, 2015). Previous research demonstrates that cybersecurity awareness strongly influences cybersecurity behaviours (Lee and Kim, 2023; Li *et al.*, 2016, 2022). Finally, based on the previous discussion, we assume that employees who intend to comply with information security policies are more likely to be aware of cybersecurity risks, leading to the implementation of preventive measures. Thus, the seventh and eighth hypotheses are posited:

H7. Intention towards ISPC is positively related to employee protective behaviour.

H8. Cybersecurity awareness is positively related to employee protective behaviour.

Figure 1 depicts our research model, comprising the eight hypotheses on incorporating IG with PMT and TPB. In the model, cybersecurity awareness is a second-order construct consisting of three first-order constructs: perceived barriers, self-efficacy and response efficacy. By establishing cybersecurity awareness as a second-order construct, this study differs from previous studies discussed in the literature review.

3. Methodology

3.1 Measurement

The survey instrument in this paper was developed based on existing literature. The questionnaire items are evaluated using a seven-point Likert scale, ranging from 1 (strongly disagree) to 7 strongly agree). The scales used for measurement are adapted from previous research. In particular, the provision of policies and SETA programmes was measured with scales adapted from previous study (Hina et *al.*, 2019), and intention towards ISPC was measured with scales adapted from prior studies (Hina et al., 2019; Ifinedo, 2012). To measure cybersecurity awareness, self-efficacy was adapted with a seven-item scale from previous research (Hina et al., 2019; Ifinedo, 2014; Li et al., 2019); response efficacy was adapted with a ten-item scale from previous studies (Hina et al., 2019; Ifinedo, 2012; Li et al., 2019; Vance et al., 2012; Wong et al., 2022); and perceived barriers were

adapted from Li et *al.* (2019). The attitude was measured with a three-item scale adapted from Hina et al. (2019) and Ifinedo (2014). Finally, employee protective behaviour was adapted with a three-item scale from Li *etal.* (2019). Appendix Table A1 describes the items measured in further detail.

3.2 Data collection

Between October 2022 and April 2023, self-administered survey forms were distributed to a diverse group of employees at the firm in major urban areas and provinces in Vietnam. We distributed a total of 750 questionnaires, of which 594 were returned, for a response rate of 79.2%, and among the returned questionnaires, 323 were considered suitable for inclusion in the study. The adequacy of the sample size was determined based on the study conducted by Hair et *al.* (2014). Questionnaires that fail to meet any of the following standards are deemed invalid and subsequently discarded. Two conditions might indicate potential issues with the survey data: first, if all respondents provide identical responses to all questions, such as selecting either the lowest or highest rating option for each item; second, if respondents complete the questionnaire in less than 2 min, as identified by Collier and Sherrell (2009).
This study uses a t-test to evaluate the demographic characteristics of the initial and final respondents, as recommended by previous studies, to minimise any potential nonresponse bias (Collier and Sherrell, 2009; Han et al., 2017). Based on the absence of observable distinctions between the two cohorts of participants, nonresponse bias does not appear to

pose a significant concern. Table 1 provides an overview of the basic information about the respondents and their respective firms.

4. Results

Partial least squares-structural equation model approach (PLS-SEM) is used to answer research questions by examining the interrelationships between the dependent, mediating and independent variables. In evaluating connections among the variables, PLS-SEM considers the precision of the measurements and how well the data match the conceptual model.

4.1 Measurement model assessment

R2 indicates how well the sample predicts the endogenous variables. An acceptable threshold value is 0.13, and a high value is 0.26 (Hair *et al.*, 2019). *R2* for cybersecurity awareness, cybersecurity compliance attitude, intention towards ISPC and employee protective behaviour is 0.636,0.162,0.570 and 0.468, respectively. Therefore, the results are satisfactory.

Table 2 shows the critical coefficients for evaluating convergence and discriminant validity. First, the factor loadings of the measurement variables were calculated to evaluate their convergent validity. Convergence validity is satisfied because the factor loading score of each item is greater than the threshold of 0.5 (Hair *et al.*, 2010). Second, Cronbach's alpha is a statistic used to assess the reliability and validity of a measurement instrument. The coefficients for each of the structures exceed the criterion of 0.6 (Hair *et al.*, 2010). Next, composite reliability (CR) values are above the cutoff of 0.70, indicating that the measurement model is trustworthy and consistent. Finally, average extracted variance (AVE) is used to evaluate the discriminant validity. In particular, the discriminant validity of the constructs is confirmed because the AVE values are above the 0.5 cutoff (Hair *et al.*, 2010).

The criterion of Fornell and Larcker and the heterotrait-monotrait (HTMT) ratio were evaluated to establish discriminant validity. The discriminant validity using HTMT should have a value of less than 0.90 for the correlation between the constructs to demonstrate the absence of a discriminant issue (Henseler *et al.*, 2015). Table 3 illustrates that all indicators of the constructs generated are less than 0.9. Moreover, using the square root of the AVE, as suggested by Fornell and Larcker, we confirm the instrument's discriminant validity (Fornell and Larcker, 1981). Table 3 shows that the AVE's square root has higher

Demographic characteristics	Category	*n* = 323	%
Gender	Male	217	67.18
	Female	106	32.82
Age	18-30 years	52	16.10
	31-40	184	56.97
	Over 40 years	87	26.93
Education level	High school	66	20.43
	Undergraduate	187	57.89
	Postgraduate	70	21.67
Years of experience	Less than 3 years	49	15.17

	3-5 years	67	20.74
	More than 5 years	207	64.09
Organisational scale	Less than 50 employees	97	30.03
	51-100 employees	68	21.05
	More than 100 employees	158	48.92

Table 1. Key characteristics of respondents

Source: Created by the authors

Table 2. Measurement assessment

Created by the authors discriminant validity than any of the other components, thus indicating satisfactory discriminant validity.

4.2 Common method bias Several scholars have discovered that complete collinearity can be used to detect common method bias (CMB). Following Kock (2015), if the full collinearity value (FCVIF) is below 3.3,

Construct	ATT	EPB	ISPC	PB	PP	RE	SETA	SE
HTMT ratio								
Cybersecurity compliance attitude (ATT) Employee protective behaviour (EPB)	0.467							
Intention towards ISPC (ISPC)	0.540	0.726						
Perceived barriers (PB)	0.031	0.030	0.055					
Provision of policies (PP)	0.487	0.743	0.733	0.063				
Response efficacy (RE)	0.495	0.733	0.779	0.072	0.809			
SETA programmes (SETA)	0.378	0.730	0.714	0.073	0.889	0.774		
Self-efficacy (SE)	0.303	0.720	0.646	0.070	0.682	0.798	0.743	
Fornell-Larcker criterion								
Cybersecurity compliance attitude (ATT)	*0.900*							
Employee protective behaviour (EPB)	0.425	*0.924*						
Intention towards ISPC (ISPC)	0.491	0.676	*0.912*					
Perceived barriers (PB)	-0.016	-0.007	-0.021	*0.826*				
Provision of policies (PP)	0.441	0.683	0.682	-0.058	*0.904*			
Response efficacy (RE)	0.449	0.689	0.731	-0.037	0.760	*0.805*		
SETA programmes (SETA)	0.348	0.682	0.675	-0.068	0.840	0.745	*0.926*	
Self-efficacy (SE)	0.282	0.666	0.608	-0.079	0.638	0.763	0.707	*0.863*

Constructs	Indicators	Loadings (>0.5)	Alpha (*a* > 0.7)	CR (>0.7)	AVE (>0.5)	FCVIF (<3.3)
Provision of policies (PP)	PP1	0.890	0.925	0.927	0.817	3.033
	PP2	0.933				
	PP3	0.871				
	PP4	0.920				
SETA programmes (SETA)	SETA1	0.927	0.959	0.960	0.858	3.099
	SETA2	0.931				
	SETA3	0.943				
	SETA4	0.928				
	SETA5	0.903				
Cybersecurity awareness (CSA)						
Response eff**i**cacy (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				
Self-eff**i**cacy (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				
Perceived barriers (PB)	PB1	0.753	0.830	1.177	0.683	1.045
	PB2	0.742				
	PB3	0.965				
Intention towards ISPC (ISPC)	ISPC1	0.879	0.932	0.934	0.832	1.542
	ISPC2	0.924				
	ISPC3	0.939				
	ISPC4	0.905				
Cybersecurity compliance attitude (ATT)	ATT1	0.893	0.883	0.884	0.810	1.334
	ATT2	0.911				
	ATT3	0.869				
Employee protective behaviour (EPB)	EPB1	0.915	0.914	0.925	0.854	1.140
	EPB2	0.940				
	EPB3	0.916				

Note: The square roots of the AVEs are shown in *italics* on the diagonal **Source:** Created by the authors

then the data have no concerns related to collinearity. Table 2 demonstrates that all the latent constructs in the data have an FCVIF value of less than 3.3, signifying the absence of CMB issues.

The results of the hypotheses tests are presented in Table 4. The findings show that all eight hypotheses are accepted at a significant level. In addition, indirect effects were estimated to determine the mediating impacts of ISPC and the cybersecurity compliance attitude on the relationships among CSA, ISPC, cybersecurity compliance attitude and employee protective behaviour. As a result, Table 5 illustrates that cybersecurity compliance attitude partially mediates the association between CSA and intention towards ISPC. Moreover, ISPC partially mediates the relationships between ATT and EPB as well as CSA and EPB.

5. Discussions

This study enhances comprehension of the elements that contribute to ISPC and protective behaviour at businesses by creating and assessing a research model combining two current

Hypothesis	*b*	*t*-value	p-value	Result

H1.PP ! CSA	0.348	3.182	0.001	Supported
H2. SETA ! CSA	0.483	4.755	0.000	Supported
H3. CSA ! ISPC	0.722	13.780	0.000	Supported
H4. CSA ! ATT	0.403	4.852	0.000	Supported
H5. ATT ! ISPC	0.239	3.274	0.001	Supported
H6. ATT ! EPB	0.270	3.673	0.000	Supported
H7. ISPC ! EPB	0.616	8.080	0.000	Supported
H8. CSA ! EPB	0.494	4.852	0.000	Supported

Table 4. Hypothesis test results

Source: Created by the authors

theoretical frameworks. It adds to the literature on cybersecurity by creating a conceptual framework for promoting cyber-safe practices in the workplace and addresses a gap in knowledge by integrating the TPB and the PMT within a theoretical framework. Our findings can be used by practitioners to enhance their efforts to inspire adherence to safety protocols by employees.

5.1 Institutional governance in raising cybersecurity awareness

Our findings build on current knowledge by highlighting the significance of effective institutional governance in increasing employee awareness regarding cybersecurity. The results indicate that implementing well-designed policies might boost people's understanding of cybersecurity concerns, implying that effective laws could increase awareness of these threats. The primary goal is to ensure that employees have the necessary knowledge and confidence to implement these security measures and are firmly convinced that adhering to these standards would help in preventing security breaches. This result aligns with the findings in previous studies on the impact of policies on cybersecurity awareness (Chan *etal.,* 2005; Hwang *et al.,* 2021; Zwilling *et al.,* 2022). Similarly, our findings demonstrate a clear association between SETA programmes and increased knowledge and understanding about cybersecurity. Employees are more likely to adopt safety precautions if they have a comprehensive understanding and awareness of the challenges associated with identifying instances of misuse. This finding is likewise in line with those in previous studies (D'Arcy *et al.,* 2009; McCrohan *etal.,* 2010; Posey *etal,* 2015; Siponen *etal,* 2009).

5.2 Importance of information security compliance in boosting employee protective behaviour According to prior findings on information security, strong awareness of the importance of compliance, security intention and attitude is critical. As shown in previous research, cybersecurity awareness and intention towards ISPC are strongly correlated (Alanazi *et al.,* 2022; Bauer and Bernroider, 2017; Dinev and Hu, 2007; Meso *et al.,* 2013; van Bavel *et al.,* 2019), cybersecurity awareness significantly impacts cybersecurity behaviours (Lee and Kim, 2023; Li *et al,* 2016, 2022). Also, cybersecurity awareness is positively related to compliance attitudes, which is consistent with previous studies (Bin-Abbas and Bakry, 2014; Dinev and Hu, 2007; Handford *etal,* 2015; Ma, 2022; Parsons *etal.,* 2014; Williams, 2008). Therefore, it is imperative for managers to be aware of the importance of employee compliance with ISPC.

The results of this study demonstrate a correlation between attachment and attitudes regarding the intention to comply with ISPC, aligning with prior research (Dinev and Hu, 2007; Guo *et al.,* 2011; Herath and Rao, 2009; Siponen *et al.,* 2014; Swaim *et al.,* 2014). The cybersecurity compliance attitude shapes employee protective behaviour (Maalem Lahcen *et al.,* 2020; Ng *et al.,* 2009; Siponen *et al.,* 2014). Similarly, the intention towards ISPC has a positive and significant impact on employee protective behaviour, consistent with prior

Hypothesis	Type	Estimates	t-values	*p*-values	Remarks
H3. CSA ! ISPC	Direct	0.722	13.780	0.000	Supported
Csa ! ATT ! ISPC	Indirect	0.096	2.411	0.016	Complementary (partial mediation)
H6. ATT ! EPB	Direct	0.270	3.673	0.000	Supported
Att! ISPC ! EPB	Indirect	0.147	3.547	0.000	Complementary (partial mediation)
H8. CSA ! EPB	Direct	0.494	4.852	0.000	Supported
Csa ! ISPC ! EPB	Indirect	0.386	4.575	0.000	Complementary (partial mediation)

Table 5.

Mediating effects

Source: Created by the authors

findings (Swaim *et al.*, 2014). The level of intention and the likelihood of compliance are directly related. Many organisational cultures may commend the crucial principles that all employees must follow without evaluating their willingness or commitment to these ideas. When people understand the reason for an activity, they are more likely to put greater effort into carrying it out. Most employees do not have sufficient competence in their fields because of a lack of training in cybersecurity, leading to a lack of comprehension and acknowledgement of the difficulty in carrying out sustainable cybersecurity projects. Thus, firms need to improve their strategy for understanding and predicting people's actions when they have stronger behavioural intentions.

5.3 Mediating effects

The results on the partial mediation of cybersecurity compliance attitudes offer behavioural insights by emphasising the influence of attitudes on compliance intentions. First, they highlight that individual views and attitudes towards cybersecurity activities are crucial for turning awareness into specific behavioural intentions about compliance with information security policies. Second, the result that ISPC is a partial mediator implies that employees' intentions, influenced by their attitudes, play a crucial role in determining the protective behaviours they display in the workplace.

6. Theoretical and practical contributions

6.1 Theoretical contributions

The main goal of this study is to strengthen ISPC by combining security expertise, raising awareness of cybersecurity and encouraging a compliance-focused mindset to enhance employee behaviours that protect against potential attacks. This study focuses on policy provision and SETA programmes in cybersecurity literature, filling a notable gap. The structure is extensive and tailored for organisations in developing countries. The study uses a unique method by combining the PMT and the TPB to explore the connections between awareness, attitude, intention and behaviour. It examines institutional governance in the realm of cybersecurity. This research makes important theoretical contributions to the development of a cybersecurity strategy plan by integrating successful methods and suggesting enhancements in employees' preventive activity. Thus, it highlights the need for security managers to integrate security policies and resources into workplace culture to promote secure behaviours by employees.

6.2 Practical contributions

Our research findings have significant ramifications for professionals in the information security industry. First, an effective institutional governance framework should support staff involvement in activities. Managers must create and disseminate comprehensive guidelines, protocols and benchmarks for all aspects of cybersecurity. This helps employees understand their duties in protecting confidential information. Strategic managers should conduct a thorough educational campaign to improve the organisation's comprehension of these security concepts. Security events that have been disclosed outside the organisation

should be discussed in staff meetings and training sessions. Individuals who show strong dedication to following information security standards should be acknowledged for their efforts.
Second, security managers should arrange training and awareness programmes to instruct employees about the company's security procedures. Organisations should consider SETA as a motivator and stress the importance of being alert to possible dangers. Training programmes should contain examples of security breaches at other organisations that resulted from the installation of "free" software, along with various scenarios that

encompass all areas of the internet service provider. Organisations should encourage the exchange of knowledge and experiences about the handling of cyber risks and the prevention of threats. Managers can encourage employees to share their knowledge on information security using internal and external incentives.
Finally, it is essential for staff to understand potential cyber threats as part of successful information security management. Security management should highlight the benefits of ISPC for customers and organisations, while also underscoring the drawbacks of noncompliance. Monetary rewards, public acknowledgement and opportunities for career advancement might inspire individuals to participate in desirable security-related activities. Senior management should engage in strategic planning to persuade staff that information security concerns are real and have the potential to cause the firm significant harm. Information security awareness requires continual revision of awareness campaigns to adapt to the ever-evolving risks and threats. Integrating awareness initiatives fully into the company culture is essential for guaranteeing that employees are well informed. Effective information security awareness training hinges on the training's relevance and consistency.

7. Conclusion and limitations

The purpose of this research is to analyse the impact of cybersecurity awareness on employees at firms in Vietnam. These connections are emphasised through the use of a quantitative research method to analyse primary data. The protection of a company's information assets increasingly depends on employees' adherence to security regulations and protective activity. In this paper, we develop a model by combining the PMT and the TPB to define employees' tendency to comply with the information security system. The enhancement of these frameworks with an examination of institutional governance enables us to offer a comprehensive understanding of cybersecurity. This study explores the human element of information security, providing clear ways to manage and guide employee adherence to information security systems. Essentially, it offers a valuable understanding of the complex nature of protecting information assets at a company, highlighting the crucial role of employee actions and the interaction between psychological theories and institutional governance in establishing a strong information security system.
Although this study enhances our comprehension of cybersecurity, it is crucial to recognise a few significant constraints. First, our research model does not cover all critical factors, such as protective knowledge, perceived risk, training support, longitudinal field interventions, work experience, organisational culture and operations management, which may strongly influence employee protective behaviours. Therefore, future studies should consider these factors when building a research framework. Second, the study provides strong evidence of partial mediating effects, which implies that other factors or pathways might also contribute to the relationship as well. Thus, future research should perform empirical analysis to examine the fundamental elements that influence the moderating impact of other factors. Finally, this study does not distinguish between the types of business and ownership. Hence, future research should perform a cluster analysis, which might yield different results.

References

Ajzen, I. (1985), "From intentions to actions: a theory of planned behavior", *Action Control*, Springer, Berlin, pp. 11-39, doi: 10.1007/978-3-642-69746-3_2.

Ajzen, I. (1991), "The theory of planned behavior", *Organizational Behavior and Human Decision Processes*, Vol. 50 No. 2, pp. 179-211, doi: 10.1016/0749-5978(91)90020-T.

Alanazi, M., Freeman, M. and Tootell, H. (2022), "Exploring the factors that influence the cybersecurity behaviors of young adults", *Computers in Human Behavior*, Vol. 136, p. 107376, doi: 10.1016/j. chb.2022.107376.

Alghamdi, M.I. (2021), "Withdrawn: determining the impact of cyber security awareness on employee behaviour: a case of Saudi Arabia", *Materials Today: Proceedings*, doi: 10.1016/j.matpr.2021.04.093.

Allam, S., Flowerday, S.V. and Flowerday, E. (2014), "Smartphone information security awareness: a victim of operational pressures", *Computers and Security*, Vol. 42, pp. 56-65, doi: 10.1016/j. cose.2014.01.005.

Ani, U.P.D., He, H. and Tiwari, A. (2017), "Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective", *Journal of Cyber Security Technology*, Vol. 1 No. 1, pp. 32-74, doi: 10.1080/23742917.2016.1252211.

Armitage, C.J. and Conner, M. (2001), "Efficacy of the theory of planned behaviour: a meta-analytic review", *British Journal of Social Psychology*, Vol. 40 No. 4, pp. 471-499, doi: 10.1348/ 014466601164939.

Barlow, J.B., Warkentin, M., Ormond, D. and Dennis, A.R. (2013), "Don't make excuses! discouraging neutralization to reduce IT policy violation", *Computers and Security*, Vol. 39, pp. 145-159, doi: 10.1016/j.cose.2013.05.006.

Bauer, S. and Bernroider, E.W.N. (2017), "From information security awareness to reasoned compliant action", *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, Vol. 48 No. 3, pp. 44-68, doi: 10.1145/3130515.3130519.

Bin-Abbas, H. and Bakry, S.H. (2014), "Assessment of IT governance in organizations: a simple integrated approach", *Computers in Human Behavior*, Vol. 32, pp. 261-267, doi: 10.1016/j. chb.2013.12.019.

Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D. and Polak, P. (2015), "What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors", *MIS Quarterly*, Vol. 39 No. 4, pp. 837-864, doi: 10.25300/MISQ/2015/39.4.5.

Bulgurcu, L., Cavusoglu, P. and Benbasat, P. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, Vol. 34 No. 3, p. 523, doi: 10.2307/25750690.

Chan, M., Woon, I. and Kankanhalli, A. (2005), "Perceptions of information security in the workplace: linking information security climate to compliant behavior", *Journal of Information Privacy and Security*, Vol. 1 No. 3, pp. 18-41, doi: 10.1080/15536548.2005.10855772.

Chang, L.Y.C. and Coppel, N. (2020), "Building cyber security awareness in a developing country: lessons from Myanmar", *Computers and Security*, Vol. 97, p. 101959, doi: 10.1016/j.cose.2020.101959.

Chen, Y., Ramamurthy, K. and Wen, K.-W. (2015), "Impacts of comprehensive information security programs on information security culture", *Journal of Computer Information Systems*, Vol. 55 No. 3, pp. 11-19, doi: 10.1080/08874417.2015.11645767.

Collier, J.E. and Sherrell, D.L. (2009), "Examining the influence of control and convenience in a self-service setting", *Journal of the Academy of Marketing Science*, Vol. 38 No. 4, pp. 490-509, doi: 10.1007/S11747-009-0179-4/METRICS.

D'Arcy, J., Hovav, A. and Galletta, D. (2009), "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach", *Information Systems Research*, Vol. 20 No. 1, pp. 79-98, doi: 10.1287/isre.1070.0160.

Dinev, T. and Hu, Q. (2007), "The centrality of awareness in the formation of user behavioral intention toward protective information technologies", *Journal of the Association for Information Systems*, Vol. 8 No. 7, pp. 386-408, doi: 10.17705/ijais.00133.

Donalds, C. and Osei-Bryson, K.-M. (2020), "Cybersecurity compliance behavior: exploring the influences of individual decision style and other antecedents", *International Journal of Information Management*, Vol. 51, p. 102056, doi: 10.1016/j.ijinfomgt.2019.102056.

Eminagaoglu, M., Uẹar, E. and Eren, § (2009), "The positive outcomes of information security

awareness training in companies: a case study", *Information Security Technical Report*, Vol. 14 No. 4, pp. 223-229, doi: 10.1016Zj.istr.2010.05.002.

Floyd, D.L., Prentice-Dunn, §. and Rogers, R.W. (2000), "A meta-analysis of research on protection motivation theory", *Journal of Applied Social Psychology*, Vol. 30 No. 2, pp. 407-429, doi: 10.1111/ j.1559-1816.2000.tb02323.x.

Fornell, C. and Larcker, D.F. (1981), "Evaluating structural equation models with unobservable variables and measurement error", *Journal of Marketing Research*, Vol. 18 No. 1, p. 39, doi: 10.2307/3151312.

Guo, K.H., Yuan, Y., Archer, N.P. and Connelly, C.E. (2011), "Understanding nonmalicious security violations in the workplace: a composite behavior model", *Journal of Management Information Systems*, Vol. 28 No. 2, pp. 203-236, doi: 10.2753/MIS0742-1222280208.

Hair, J.F., Black, W.C., Babin, B.J. and Anderson, R.E. (2010), *Multivariate Data Analysis*, (7th ed.). Pearson, New York, NY.

Hair, J.F., Jr, Hult, G.T.M., Ringle, C.M. and §arstedt, M. (2014), "A primer on partial least squares structural equations modeling (PLS-SEM)", *European Journal of Tourism Research*, Vol. 6 No. 2, pp. 211-213.

Hair, J., Risher, J., Sarstedt, M. and Ringle, C. (2019), "When to use and how to report the results of PL§- SEM", *European Business Review*, Vol. 31 No. 1, pp. 2-24, doi: 10.1108/EBR-11-2018-0203.

Han, J.Y., Kim, Y.J. and Kim, H. (2017), "An integrative model of information security policy compliance with psychological contract: examining a bilateral perspective", *Computers and Security*, Vol. 66, pp. 52-65, doi: 10.1016/j.cose.2016.12.016.

Handford, C.E., Dean, M., Spence, M., Henchion, M., Elliott, C.T. and Campbell, K. (2015), "Awareness and attitudes towards the emerging use of nanotechnology in the agri-food sector", *Food Control*, Vol. 57, pp. 24-34, doi: 10.1016/j.foodcont.2015.03.033.

Henseler, J., Ringle, C.M. and Sarstedt, M. (2015), "A new criterion for assessing discriminant validity in variance-based structural equation modeling", *Journal of the Academy of Marketing Science*, Vol. 43 No. 1, pp. 115-135, doi: 10.1007/s11747-014-0403-8.

Herath, T. and Rao, H.R. (2009), "Protection motivation and deterrence: a framework for security policy compliance in organisations", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 106-125, doi: 10.1057/ejis.2009.6.

Hina, S., Panneer Selvam, D.D.D. and Lowry, P.B. (2019), "Institutional governance and protection motivation: theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world", *Computers and Security*, Vol. 87, p. 101594, doi: 10.1016/j.cose.2019.101594.

Hu, Q., Hart, P. and Cooke, D. (2007), "The role of external and internal influences on information systems security: a neo-institutional perspective", *The Journal of Strategic Information Systems*, Vol. 16 No. 2, pp. 153-172, doi: 10.1016/j.jsis.2007.05.004.

Hwang, I., Wakefield, R., Kim, S. and Kim, T. (2021), "Security awareness: the first step in information security compliance behavior", *Journal of Computer Information Systems*, Vol. 61 No. 4, pp. 345-356, doi: 10.1080/08874417.2019.1650676.

Ifinedo, P. (2012), "Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory", *Computers and Security*, Vol. 31 No. 1, pp. 83-95, doi: 10.1016/j.cose.2011.10.007.

Ifinedo, P. (2014), "Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition", *Information and Management*, Vol. 51 No. 1, pp. 69-79, doi: 10.1016/j.im.2013.10.001.

Janmaimool, P. (2017), "Application of protection motivation theory to investigate sustainable waste management behaviors", *Sustainability*, Vol. 9 No. 7, p. 1079, doi: 10.3390/su9071079.

Johnston, P. and Warkentin, O. (2010), "Fear appeals and information security behaviors: an empirical study", *MIS Quarterly*, Vol. 34 No. 3, p. 549, doi: 10.2307/25750691.

Kim, J., Yang, K., Min, J. and White, B. (2022), "Hope, fear, and consumer behavioral change amid COVID-19: application of protection motivation theory", *International Journal of Consumer Studies*, Vol. 46 No. 2, pp. 558-574, doi: 10.1111/ijcs.12700.

Kock, N. (2015), "Common method bias in PLS-SEM: a full collinearity assessment approach", *InternationalJournal ofE-Collaboration*, Vol. 11 No. 4, pp. 1-10.

Lee, Y. (2011), "Understanding anti-plagiarism software adoption: an extended protection motivation theory perspective", *Decision Support Systems*, Vol. 50 No. 2, pp. 361-369, doi: 10.1016/j.dss.2010.07.009.

Lee, C.S. and Kim, D. (2023), "Pathways to cybersecurity awareness and protection behaviors in South Korea", *Journal of Computer Information Systems*, Vol. 63 No. 1, pp. 94-106, doi: 10.1080/ 08874417.2022.2031347.

Lee, J. and Lee, Y. (2002), "A holistic model of computer abuse within organizations", *Information Management and Computer Security*, Vol. 10 No. 2, pp. 57-63, doi: 10.1108/09685220210424104.

Lee, K.G., Chong, C.W. and Ramayah, T. (2017), "Website characteristics and web users' satisfaction in a higher learning institution", *International Journal of Management in Education*, Vol. 11 No. 3, p. 266, doi: 10.1504/IJMIE.2017.084926.

Liao, C., Chen, J.-L. and Yen, D.C. (2007), "Theory of planning behavior (TPB) and customer satisfaction in the continued use of e-service: an integrated model", *Computers in Human Behavior*, Vol. 23 No. 6, pp. 2804-2822, doi: 10.1016/j.chb.2006.05.006.

Li, L., Xu, L. and He, W. (2022), "The effects of antecedents and mediating factors on cybersecurity protection behavior", *Computers in Human Behavior Reports*, Vol. 5, p. 100165, doi: 10.1016/j. chbr.2021.100165.

Li, L., Xu, L., He, W., Chen, Y. and Chen, H. (2016), "Cyber security awareness and its impact on employee's behavior", doi: 10.1007/978-3-319-49944-4_8.

Li, L., He, W., Xu, L., Ash, I., Anwar, M. and Yuan, X. (2019), "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior", *International Journal of Information Management*, Vol. 45, pp. 13-24, doi: 10.1016/j .ijinfomgt.2018.10.017.

McCrohan, KF., Engel, K. and Harvey, J.W. (2010), "Influence of awareness and training on cyber security", *Journal of Internet Commerce*, Vol. 9 No. 1, pp. 23-41, doi: 10.1080/15332861.2010.487415.

Ma, X. (2022), "Is professionals' information security behaviors in Chinese IT organizations for information security protection", *Information Processing and Management*, Vol. 59 No. 1, p. 102744, doi: 10.1016/j.ipm.2021.102744.

Maalem Lahcen, R.A., Caulkins, B., Mohapatra, R. and Kumar, M. (2020), "Review and insight on the behavioral aspects of cybersecurity", *Cybersecurity*, Vol. 3 No. 1, p. 10, doi: 10.1186/s42400-020-00050-w.

Maddux, J.E. and Rogers, R.W. (1983), "Protection motivation and self-efficacy: a revised theory of fear appeals and attitude change", *Journal of Experimental Social Psychology*, Vol. 19 No. 5, pp. 469-479, doi: 10.1016/0022-1031(83)90023-9.

Mahon, D., Cowan, C. and McCarthy, M. (2006), "The role of attitudes, subjective norm, perceived control and habit in the consumption of ready meals and takeaways in great Britain", *Food Quality and Preference*, Vol. 17 No. 6, pp. 474-481, doi: 10.1016/j.foodqual.2005.06.001.

Menard, P., Bott, G.J. and Crossler, R.E. (2017), "User motivations in protecting information security: Protection motivation theory versus self-determination theory", *Journal of Management Information Systems*, Vol. 34 No. 4, pp. 1203-1230, doi: 10.1080/07421222.2017.1394083.

Meso, P., Ding, Y. and Xu, S. (2013), "Applying protection motivation theory to information security training for college students", *Journal of Information Privacy and Security,* Vol. 9 No. 1, pp. 47-67, doi: 10.1080/15536548.2013.10845672.

Michael, K., Kobran, S., Abbas, R. and Hamdoun, S. (2019), "Privacy, data rights and cybersecurity: technology for good in the achievement of sustainable development goals", 2019 IEEE

International Symposium on Technology and Society (ISTAS), pp. 1-13, doi: 10.1109/ ISTAS48451.2019.8937956.

Moletsane, T. and Tsibolane, P. (2020), "Mobile information security awareness among students in higher education: an exploratory study", 2020 Conference on Information Communications Technology and Society (ICTAS), pp. 1-6, doi: 10.1109/ICTAS47918.2020.233978.

Ng, B.-Y. and Xu, Y. (2007), "Studying users' computer security behavior using the health belief model", *PACIS2007Proceedings,* pp. 423-437.

Ng, B.-Y., Kankanhalli, A. and Xu, Y. (2009), "Studying users' computer security behavior: a health belief perspective", *Decision Support Systems,* Vol. 46 No. 4, pp. 815-825, doi: 10.1016/j.dss.2008.11.010.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014), "Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)", *Computers and Security,* Vol. 42, pp. 165-176, doi: 10.1016/j.cose.2013.12.003.

Posey, C., Roberts, T.L. and Lowry, PB. (2015), "The impact of organizational commitment on insiders' motivation to protect organizational information assets", *Journal of Management Information Systems,* Vol. 32 No. 4, pp 179-214, doi: 10.1080/07421222.2015.1138374.

Rippetoe, P.A. and Rogers, R.W. (1987), "Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat", *Journal of Personality and Social Psychology,* Vol. 52 No. 3, pp. 596-604, doi: 10.1037/0022-3514.52.3.596.

Rogers, R.W. (1975), "A protection motivation theory of fear appeals and attitude change", *The Journal of Psychology,* Vol. 91 No. 1, pp. 93-114, doi: 10.1080/00223980.1975.9915803.

Roy Sarkar, K. (2010), "Assessing insider threats to information security using technical, behavioural and organisational measures", *Information Security Technical Report,* Vol. 15 No. 3, pp. 112-133, doi: 10.1016/j.istr.2010.11.002.

Saadatdoost, R., Sim, A.T.H., Jafarkarimi, H. and Mei Hee, J. (2015), "Exploring MOOC from education and information systems perspectives: a short literature review", *Educational Review,* Vol. 67 No. 4, pp. 505-518, doi: 10.1080/00131911.2015.1058748.

Safa, S.N., Von Solms, R. and Furnell, S. (2016), "Information security policy compliance model in organizations", *Computers and Security,* Vol. 56, pp. 70-82, doi: 10.1016/j.cose.2015.10.006.

Shaw, R.S., Chen, C.C., Harris, A.L. and Huang, H.-J. (2009), "The impact of information richness on information security awareness training effectiveness", *Computers and Education,* Vol. 52 No. 1, pp. 92-100, doi: 10.1016/j.compedu.2008.06.011.

Siponen, M., Adam Mahmood, M. and Pahnila, S. (2014), "Employees' adherence to information security policies: an exploratory field study", *Information and Management,* Vol. 51 No. 2, pp. 217-224, doi: 10.1016/j.im.2013.08.006.

Siponen, M., Mahmood, M.A. and Pahnila, S. (2009), "Technical opinion: are employees putting your company at risk by not following information security policies?", *Communications of the ACM,* Vol. 52 No. 12, pp. 145-147, doi: 10.1145/1610252.1610289.

Sommestad, T., Karlzen, H. and Hallberg, J. (2015), "The sufficiency of the theory of planned behavior for explaining information security policy compliance", *Information and Computer Security,* Vol. 23 No. 2, pp. 200-217, doi: 10.1108/ICS-04-2014-0025.

Straub, D.W. (1990), "Effective is security: an empirical study", *Information Systems Research*, Vol. 1 No. 3, pp. 255-276, doi: 10.1287/isre.1.3.255.

Swaim, J.A., Maloni, M.J., Napshin, S.A. and Henley, A.B. (2014), "Influences on student intention and behavior toward environmental sustainability", *Journal of Business Ethics,* Vol. 124 No. 3, pp. 465-484, doi: 10.1007/s10551-013-1883-z.

Teo, T. and Beng Lee, C. (2010), "Explaining the intention to use technology among student teachers", *Campus-Wide Information Systems,* Vol. 27 No. 2, pp. 60-67, doi: 10.1108/10650741011033035.

Tran, D.V., Nguyen, P., Van-Nguyen, A.T.C., Vrontis, D. and Dinh, P.U. (2024), "Exploring the influence of government social media on cybersecurity compliance: employee attitudes, motivation and behaviors", *Journal of Asm Business Studies,* Vol. 18 No. 1, pp. 204-223, doi: 10.1108/JABS-09- 2023-0343.

Tsai, H.S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N.J. and Cotten, S.R. (2016), "Understanding online safety behaviors: a protection motivation theory perspective", *Computers and Security,* Vol. 59, pp. 138-150, doi: 10.1016/j.cose.2016.02.009.

Tsohou, A., Karyda, M. and Kokolakis, S. (2015), "Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs", *Computers and Security,* Vol. 52, pp. 128-141, doi: 10.1016/j.cose.2015.04.006.

Van Bavel, R., Rodríguez-Priego, N., Vila, J. and Briggs, P. (2019), "Using protection motivation theory in the design of nudges to improve online security behavior", *International Journal of Human-Computer Studies*, Vol. 123, pp. 29-39, doi: 10.1016/j.ijhcs.2018.11.003.

Vance, A., Siponen, M. and Pahnila, S. (2012), "Motivating is security compliance: insights from habit and protection motivation theory", *Information and Management*, Vol. 49 Nos 3/4, pp. 190-198, doi: 10.1016/j.im.2012.04.002.

Venkatesh, M., Davis, P. and Davis, L. (2003), "User acceptance of information technology: toward a unified view", *MIS Quarterly*, Vol. 27 No. 3, pp. 425-478, doi: 10.2307/30036540.

Wall, JD. and Warkentin, M. (2019), "Perceived argument quality's effect on threat and coping appraisals in fear appeals: an experiment and exploration of realism check heuristics", *Information and Management*, Vol. 56 No. 8, p. 103157, doi: 10.1016/j.im.2019.03.002.

Whitman, M.E. (2003), "Enemy at the gate", *Communications of the ACM*, Vol. 46 No. 8, pp. 91-95, doi: 10.1145/859670.859675.

Wiafe, I., Koranteng, F.N., Wiafe, A., Obeng, E.N. and Yaokumah, W. (2020), "The role of norms in information security policy compliance", *Information and Computer Security*, Vol. 28 No. 5, pp. 743-761, doi: 10.1108/ICS-08-2019-0095.

Williams, P.A.H. (2008), "In a 'trusting' environment, everyone is responsible for information security", *Information Security Technical Report*, Vol. 13 No. 4, pp. 207-215, doi: 10.1016/j.istr.2008.10.009.

Wong, L.-W., Lee, V.-H., Tan, G.W.-H., Ooi, K.-B. and Sohal, A. (2022), "The role of cybersecurity and policy awareness in shifting employee compliance attitudes: building supply chain capabilities", *International Journal of Information Management*, Vol. 66, p. 102520, doi: 10.1016/j. ijinfomgt.2022.102520.

Workman, M. (2009), "A field study of corporate employee monitoring: attitudes, absenteeism, and the moderating influences of procedural justice perceptions", *Information and Organization*, Vol. 19 No. 4, pp. 218-232, doi: 10.1016/j.infoandorg.2009.06.001.

Wu, X. and Kuang, W. (2021), "Exploring influence factors of WeChat users' health information sharing behavior: based on an integrated model of TPB, UGT and SCT", *International Journal of Human-Computer Interaction*, Vol. 37 No. 13, pp. 1243-1255, doi: 10.1080/10447318.2021.1876358.

Yousuf, H., Al-Emran, M. and Shaalan, K. (2023), "Evaluating individuals' cybersecurity behavior in mobile payment contactless technologies: extending TPB with cybersecurity awareness", *International Conference on Human-Computer Interaction*, pp. 542-554, doi: 10.1007/978-3-031- 35822-7_35

Zhang, J., Reithel, B.J. and Li, H. (2009), "Impact of perceived technical protection on security behaviors", *Information Management and Computer Security*, Vol. 17 No. 4, pp. 330-340, doi: 10.1108/09685220910993980.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek-Cetin, F. and Basim, H.N. L. (2022), "Cyber security awareness, knowledge and behavior: a comparative study", *Journal of Computer Information Systems*, Vol. 62 No. 1, pp. 82-97, doi: 10.1080/08874417.2020.1712269.

Appendix

Provision of policies (PP)	PP1	My organisation has established behavioural rules for computer use according to state regulations My	Minor
	PP2	organisation has guidelines for the use of computers within the organisation that comply with the regulations	Minor
	PP3	A policy has been established to prohibit employees from accessing documents on computers that they are not authorised to use, according to state regulations My organisation has de**fi**ned a code	Minor
	PP4	of conduct outlining the information security with which everyone must comply	Minor
SETA programmes (SETA)	SETA1	My organisation frequently conducts brie**fi**ngs on the topic of security violations through awareness campaigns (e-mail, brochure/seminar/workshops) My organisation	Minor
	SETA2	provides regular updates for me on	Minor

		the latest threats to computer systems and how to protect myself	
	SETA3	My organisation provides employees with continuing training on their role in maintaining computer security	Minor
	SETA4	The information security educational sessions at my organisation have prepared me to be fully informed about cybersecurity hazards	Minor
	SETA5	The programs that raise awareness about information security at my organisation help me learn the required skills to adopt protective behaviour	Minor
Self-ef**fi**cacy (SE)	SE1	I am con**fi**dent that I have enough essential skills to safeguard against any breaches of information security	Minor
	SE2	I am con**fi**dent that I can keep my information privacy safe through my own efforts	Minor
	SE3	I employ security protocols (**fi**rewall, antivirus, etc.) on my work-related computers	Minor
	SE4	I have con**fi**dence in my ability to shield myself from breaches in information security	Minor
	SE5	I am comfortable adjusting the security level in my web browser	Minor
	SE6	I believe that I can deal with **fi**les that are infected with viruses	Minor
	SE7	I am con**fi**dent in my ability to eliminate spyware and malware from my computer	Minor
Perceived barriers (PB)	PB1	Verifying an email with attached **fi**les is inconvenient	Minor
	PB2	Making changes to personal privacy settings on social networking platforms is inconvenient	Minor
	PB3	Regularly backing up a computer is inconvenient	Minor
Intention towards ISPC (ISPC)	ISPC1	I intend to safeguard information resources and technology in accordance with the organisation's information security policies	Minor
	ISPC2	In the future, I intend to comply with the rules laid down in the organisation's information security policies	Minor
	ISPC3	In the future, I intend to ful**fi**l my duties regarding information security policies	Minor
	ISPC4	I intend to uphold my commitment to complying with the organisation's information security policies	Minor
Cybersecurity compliance attitude (ATT)	ATT1	Complying with the information security policies of my organisation is crucial	Minor
	ATT2	I believe it is reasonable to adhere to information	Minor

		security policies	
	ATT3	Following the information security policies of my organisation is a commendable idea	Minor
Employee protective behaviour (EPB)	EPB1	My computer always has the latest antivirus software installed	Minor
	EPB2	I keep an eye out for unusual activity on the computer (e.g. computer slowing down or freezing up, pop-up windows)	Minor
	EPB3	I immediately act on any warnings about malware	Minor

Unraveling influential factors shaping employee cybersecurity behaviors: an empirical investigation of public servants in Vietnam

Dien Van Tran, Phuong Van Nguyen, Demetris Vrontis, Sam Thi Ngoc Nguyen and Phuong Uyen Dinh

Abstract

Purpose - *Government employees must comply with policies on information security regulations, online security practices, social networking usage, internet addiction, online cyberthreats and other related habits. These activities are considered cybersecurity behaviors. Government social media (GSM) accounts are increasingly used to educate employees about cybersecurity risks. To support the effectiveness of cybersecurity practices in government organizations, the purpose of this study is to investigate the impacts of GSM and organizational policy compliance on employees' cybersecurity awareness, motivation and behaviors.*

Design/methodology/approach - *Data were obtained by administering a questionnaire survey to public personnel in Vietnam. A total of330 valid responses were obtained, and the research hypotheses were tested using partial least squares-structural equation modeling.*

Findings - *First, cybersecurity awareness enhances information protection motivation and employee protective behavior. Second, GSM has positive impacts on cybersecurity knowledge and information protection motivation. Third, there is a strong positive association between information protection motivation and employee protective behavior. Finally, while organizational compliance significantly increases cybersecurity awareness, its impacton employee protective behavior is ind irect.*

Originality/value - *This research enhances the literature on the behavioral dimension of cybersecurity. The primary objective of this study is to assess the influence of cybersecurity awareness on protective behaviors rather than intents and attitudes alone. Furthermore, this research integrates protection motivation theory and cultivation theory to provide a more thorough assessment of cybersecurity awareness and protective behavior. By investigating the impact of GSM on the level of cybersecurity awareness among employees within government organizations, this study provides valuable insights into the efficacy of recent governmental initiatives aimed at fostering cybersecurity.*

Keywords *Organizational policy compliance, Government social media, Cybersecurity awareness, Information protection motivation, Employee protective behavior*

Paper type *Research paper*

1. Introduction

Information and communication technologies (ICT) have become deeply integrated within national infrastructures and nearly all aspects of daily life (Li *et al.*, 2022). The unprecedented penetration of ICT has helped organizations gain competitive advantages through improvements in system accessibility, communication speed and efficiency and reduced operating costs (Hasan *et al.*, 2021). The adoption of digital finance has been more influenced by its potential benefits than by its perceived risks (Jain and Raman, 2023). Nonetheless, digital advancements can pose serious cybersecurity threats to organizations because of their dynamic features, complex multifunctionality and interconnectedness (Fosch-Villaronga and Mahler, 2021; Li *eta/.*, 2019). Cyberattacks on businesses of all sizes and industries are increasing in frequency, volume and sophistication (Lu and Xu, 2019). Cyberattacks can cause severe damage to organizations by intentionally or unintentionally exposing

confidential information (Ou eta/., 2022). However, there are significant gaps in our understanding of the variations in cybersecurity awareness, knowledge and behavior among employees.

The best way to reduce the threat of cyberattacks is to increase individual awareness. The term "cybersecurity awareness" refers to the extent to which individuals understand the significance of information security and their obligations to implement adequate levels of information security control to safeguard an organization's data and networks (Shaw *eta/.,* 2009). Most individuals do not fully understand which instruments are required for protection against cyber risks (Zwilling *et a/.,* 2022). In addition, as the world becomes increasingly digitally interconnected, the most effective strategy for enhancing cybersecurity awareness is to improve the know-how of both citizens and employees in the business and public administration sectors (Zwilling *eta/.,* 2022). To do so, organizations must establish policy compliance. Organizational policy compliance refers to the extent to which individuals conform to the prescribed rules, regulations, standards and guidelines of an organization. Organizational policies generally encompass a broad spectrum of domains, including but not limited to code of conduct, information security, data privacy, safety standards and human resources practices. Adherence to organizational policies guarantees uniformity, equity and legality in the activities and conduct of employees or members of the organization (AlKalbani *eta/.,* 2017; Bauer *eta/.,* 2017). However, empirical studies of the relationships between organizational policy compliance with cybersecurity awareness and employee protective behavior have yielded conflicting findings (Lee *eta/.,* 2004; Lee and Larsen, 2009; Li *eta/.,* 2019). Investigating these relationships in the public sector of an emerging market, such as Vietnam, has the potential to add new insights.

Moreover, the role of protection motivation is significant in influencing employee behaviors pertaining to compliance with information security policies. Particularly, information protection motivation is the degree of employees' motivation to implement preventive measures against cyberattacks (Ma, 2022; Posey *eta/.,* 2015; Vrhovec and Mihelic, 2021). This motivation is the result of threat appraisal and coping appraisal processes and operates as an intervening variable similar to other motives that induce, sustain and direct employees' activities (Martens *eta/.,* 2019). According to the protection motivation theory (PMT), employees will take measures to protect themselves against cybersecurity risks when they see a threat and believe they possess the necessary abilities to handle the potential danger. However, individuals frequently have an insufficient awareness or understanding of how to safeguard themselves against cyberattacks (Klein and Zwilling, 2023). Employee protective behaviors are the steps that employees take to correctly address cybersecurity concerns (Li *eta/.,* 2019; Tang *eta/.,* 2021).

An organization's information security system is affected by many factors at the individual and organizational levels. Behavioral factors have recently been the focus of attention because employees directly control the accessibility, confidentiality and integrity of information (Ma, 2022). More than 70% of security breaches are because of employee negligence or inadequate compliance with organizational cybersecurity protocols (Alshaikh *et a/.,* 2021). In some cases, employees are not sufficiently aware of the variety of attacks that are constantly altering the corporate security landscape (Zwilling *et a/.,* 2022). For example, opening an email with an unfamiliar file extension or providing illegal access to others has the potential to expose the entire organization to cybersecurity breaches. In addition, employees tend to overlook mandatory security measures when completing tasks (Ifinedo, 2012), especially when managing multiple tasks simultaneously and facing stringent deadlines (Chowdhury *eta/.,* 2019). Thus, given the important role of employees in

cybersecurity, the government and organizations should examine and prioritize practices that effectively enhance employees' awareness and protective behaviors.

Social media encompasses apps and social network platforms that are part of Web 2.0 technology. These platforms enable the development, diffusion and transmission of knowledge across communities of users (Del Vecchio *et al.,* 2020). The growing popularity of social media influencers has led to the widespread adoption of influencer marketing in business strategies (Vrontis et *al.,* 2021). Government social media (GSM) accounts enhance the dissemination of official information and provide new platforms that are accessible and beneficial to the general public (Islm *etal.,* 2021). Specifically, GSM is the online presence established and overseen by a governmental department or organization across various social media platforms (Tang *et al.,* 2021). Governments can use GSM to quickly provide information to citizens, keep them aware of the status of threats, prevent the spread of false data and provide assistance to victims of disasters (Guo *etal.,* 2021).

Specifically, studies of GSM have primarily focused on citizens' reasons for interacting with GSM and categorizing emergency messaging strategies (Tang *et al.,* 2021). The impact of GSM on citizens during acute outbreaks of disease, such as COVID-19 or measles, has also been explored. However, there is a notable gap in understanding the impact of GSM on persistent issues spanning decades, such as cybersecurity attacks. A comprehensive understanding of these effects from a behavioral perspective will help GSM operators formulate effective engagement strategies and craft valuable messages. Likewise, governments can use social media accounts to increase awareness of cybersecurity threats, but the effectiveness of these efforts

has not been established. Importantly, limited research has been conducted on the expansion of cultivation theory within the framework of GSM.

To address the above gaps, this study integrates PMT and cultivation theory to examine the effects of individual factors (awareness and motivation), organizational factors (cybersecurity policy) and GSM on employees' protective behaviors related to cybersecurity. The following research questions are addressed:

RQ1. How do organizational policies affect employees' cybersecurity awareness and behaviors?

RQ2. How does government social media influence employees' cybersecurity awareness and protective behaviors?

RQ3. How does employees' cybersecurity awareness affect their protective behaviors?

The broad expansion of internet accessibility has significantly increased the complexity and frequency of cyberattacks, with extensive adverse consequences in multiple sectors, including businesses, industries and political administrations. In the face of these growing dangers, governments around the world have taken specific actions to strengthen the security of networks, especially those that are crucial for national defense. In Vietnam, cyberattacks mainly target key information infrastructures of central authorities and large financial corporations. Enhancing the legal structure that regulates network information security can help safeguard critical national defense information. A crucial component of this undertaking is evaluating the capacity and operational knowledge of network overseers, as efficiently protecting against cyberattacks requires proficient staff. Furthermore, the proper management of network information security depends on a comprehensive regulatory framework to reduce risks and effectively address cyberthreats. The Cybersecurity Law of Vietnam, which was implemented on January 1, 2019, highlights the government's dedication to maintaining societal order and safety in cyberspace. This legislation clearly outlines the duties and obligations of pertinent authorities, companies and individuals. However, additional studies of guidelines and organizational policy compliance are needed to guarantee the safety and security of employees as they navigate the digital realm, specifically in relation to internet usage and online transactions. In Vietnam, social media platforms are widely used by government organizations and officials, and the predominant platforms for GSM are Facebook, Zalo, Viber, YouTube, TikTok and Instagram.

This study contributes significantly to the literature on cybersecurity in Vietnam, especially behavioral aspects, by measuring the effects of cybersecurity awareness on actual protective behaviors rather than merely behavioral intentions, attitudes and likelihood. In addition, by integrating four components of the PMT and cultivation theory into the assessment of cybersecurity awareness, this study provides comprehensive measurements of the awareness of both threats and available countermeasures. Moreover, the influence of GSM on cybersecurity awareness among organizational insiders is investigated to provide insights into the effectiveness of recent government efforts to promote cybersecurity. Finally, by considering the information security context of the public sector, this research provides a foundation for the top management of public organizations to make strategic decisions about the governance, use and operation of computer systems and networks.

The remainder of the study is structured as follows. Section 2 reviews the literature and presents the theoretical framework, variable definitions, proposed hypotheses and the research model. Section 3 outlines the methodology for addressing the research questions, while Section 4 provides the results and discussion. Section 5 concludes with theoretical contributions, research implications and limitations.

2. Literature review

2.1 Protection motivation theory

The PMT is a widely acknowledged theoretical framework for evaluating behaviors intended to mitigate the adverse consequences of perceived threats (Li *et al.*, 2022). This theory explains that attitude change is contingent on the level of protective motivation generated from the cognitive appraisal process, which includes perceived severity, perceived vulnerability, self-efficacy and response efficacy (Maddux and Rogers, 1983). Perceived severity refers to the perceived magnitude, danger and consequences of a manifest threat such as computer viruses, unauthorized access or internet hacking (Hina *et al.*, 2019; Li et *al.*, 2022). Perceived vulnerability reflects an individual's perception of the likelihood of a threat occurring or of being exposed to a threat (Hina et *al.*, 2019; Li et *al.*, 2019; Wong *et al.*, 2022). Self-efficacy pertains to an individual's judgment of the capabilities and skills required to execute recommended protective behaviors for coping with

threats, such as eliminating spyware from electronic devices or handling virus-infected files (Hina et *al.*, 2019; Li et *al.*, 2022). Response efficacy relates to the perceived effectiveness of countermeasures against cyberattacks that an employee can implement to prevent a potential threat (Hina *etal.*, 2019; Li *etal.*, 2019; Wong *etal.*, 2022).

The PMT was originally developed in the health domain (Floyd *etal.*, 2000) but has since been extended to other fields, including computer and information security (Boss *et al.*, 2015). The PMT has been used to explain general users' predominant information security behaviors (van Bavel *etal.*, 2019). It has also been used to analyze individual information security practices in various settings, such as households (Martens *et al.*, 2019), higher education organizations (Hina *etal.*, 2019; Hina and Dominic, 2020) and business organizations (Li *et al.*, 2019). The PMT is especially advantageous in the organizational context, where employees and end-users require additional encouragement to safeguard their valuable data assets (Li *et al.*, 2022). Here, we use the PMT to investigate the determinants of protective behaviors among public servants in governmental organizations, an understudied segment.

2.2 Cultivation theory

Cultivation theory is a communication theory that describes how mass media coverage shapes the public's opinions of social phenomena (Gerbner and Gross, 1976). Cultivation theory posits that a persistently high frequency of media consumption will increase the alignment of an individual's perceptions of social realities with media depictions (Tang *etal.*, 2021). Cultivation is a continual and dynamic process that includes two forms: mainstreaming and resonance (Hermann et *al.*, 2020). Mainstreaming refers to the convergence of different views as a result of content exposure, while resonance occurs when media content is highly relevant to real-life experiences (Hermann *et al.*, 2020). The cultivation approach originally focused on television but can be applied to any dominant medium, especially social media, that strengthens perceptions and attitudes by providing an accessible, engaging and shared symbolic environment (Intravia *etal.*, 2017). GSM has attracted attention as a means of cultivation (Tang *etal.*, 2021). Compared to conventional government Web portals, social media is a more efficient means of distributing information and fostering two-way interaction (Guo *etal.*, 2021).

Both the PMT and cultivation theory are suitable for this study. This study expands the scope of these theories to examine civil servants' assessment of cybersecurity awareness and protective behavior.

2.3 Hypothesis development

2.3.1 Cybersecurity awareness, information protection motivation and employee protective behavior. Although research on cybersecurity awareness is growing, there is no single construct; researchers have considered several dimensions of cybersecurity awareness (Hanus *et al*, 2018). Defining cybersecurity awareness is a prerequisite for increasing cybersecurity awareness (Zwilling *et al.*, 2022). Several prior studies have used the PMT to conceptualize cybersecurity awareness but have not explicitly defined the construct (Lee and Larsen, 2009; Vance *et al.*, 2012). In this study, we adopt a threat perspective and consider cybersecurity awareness a second-order construct comprising four components: perceived severity, perceived vulnerability, self-efficacy and response efficacy. Thus, cybersecurity awareness is the state where employees are conscious of the occurrence and nature of cybersecurity threats, the potential effects of cybersecurity threats on organizational security (perceived severity and perceived vulnerability), their own capabilities and the expected measures for preventing such threats (self-efficacy and response efficacy).

According to the PMT, the level of elicited protection motivation is contingent on appraisals of perceived severity, perceived vulnerability, self-efficacy and response efficacy (Maddux and Rogers, 1983). If a threat is perceived as non-severe or improbable, if no viable action can be implemented to mitigate it or if the individual doubts their ability to cope with the situation, then protection motivation will not be aroused, and behavioral intentions will not change. Therefore, cybersecurity awareness should have a direct influence on the motivation for protective action:

H1. Cybersecurity awareness has a positive impacton information protection motivation.

According to the PMT, employees who are more aware of cyberthreats are more likely to learn how to secure their devices, leading to stronger cyber-protective behavior (Klein and Zwilling, 2023). Examples of protective behaviors include regularly changing passwords, adhering to organizational standards, exercising caution before clicking on links from unknown sources, backing up data, patching software and deploying cybersecurity defense tools (Posey *et al.*, 2015; Tang *et al.*, 2021). By contrast, risky behaviors include activities such as disclosing personal passwords, downloading unlawful content, violating copyright regulations and neglecting suggested software updates (Zwilling *et al.*, 2022). Previous research has shown direct effects of cybersecurity awareness on the prevention of information system misuse (D'Arcy *et al.*, 2009) and compliance with cybersecurity policy (Bulgurcu *et al.*, 2010). High cybersecurity awareness significantly increases employees' knowledge of

security threats and system vulnerabilities and, in turn, their vigilance against potential cyberattacks, thus ensuring that the information, systems and networks they engage with are protected (Corallo *et al.*, 2022). The greater the perceived severity and perceived vulnerability of a potential threat to their organization's cyber assets, the greater the likelihood that employees will adopt protective behaviors and vice versa (Martens *etal.*, 2019). Likewise, if an employee has strong confidence in a coping mechanism's effectiveness and their ability to execute that protective measure, then they will be more inclined to act (Li *etal.*, 2022; Tang *etal.*, 2021). Thus, we propose the following:

H2. Cybersecurity awareness has a positive impact on employee protective behavior.

2.3.2 Information protection motivation and employee protective behavior Some scholars have reframed information protection motivation as an attitude, while others omit information protection motivation and directly examine the predictive value of (intention toward) protective behavior (Wu, 2020). Few studies have examined the link between protection motivation and actual behaviors. While the primary aim of the PMT is to assess protection motivation, it can be extended to evaluate actual protective behaviors (Ma, 2022). As the ultimate goal of cybersecurity research is to enhance security practices instead of merely intentions, assessing actual behaviors is valuable. In addition, a meta-analysis of the PMT showed that protection motivation is the strongest predictor of behavioral changes (Boss *et al.*, 2015). Thus, we extend the PMT by integrating employee protective behavior and hypothesize the following:

H3. Information protection motivation has a positive impact on employee protective behavior.

2.3.3 Government social media and cybersecurity awareness According to cultivation theory, media consumption can shape an individual's perceptions and opinions (Hermann *et al.*, 2020). GSM participation encompasses the interactive engagement of GSM followers through behaviors such as viewing, commenting and exchanging cybersecurity-related messages inside the GSM network (Tang *et al.*, 2021). GSM participation can be seen as a form of media consumption because it contributes to enhancing people's situational awareness of a cyber crisis (Guo *et al.*, 2021). Individuals who actively engage with GSM messages regarding cybersecurity are more likely to develop heightened cybersecurity awareness (Tang *et al.*, 2021). More precisely, the government's regular dissemination of cybercrime-related news frequently results in elevated levels of perceived threat among the public. This is because individuals tend to believe that events shown in the media have the potential to impact them or their loved ones (Intravia *et al.*, 2017; Shah *et al.*, 2020). Moreover, participation in GSM equips individuals with timely information and guidance to respond effectively to potential threats (Farooq *et al.*, 2020), providing a foundation for evaluating the efficacy of protective responses (Tu *etal.*, 2015). In addition, this advanced preparedness will increase individuals' confidence in their ability to protect themselves from threats (Tang *etal.*, 2021). Thus, we propose the following:

H4. Government social media has a positive impact on cybersecurity awareness.

For an individual to be motivated to take an action, they must understand the purpose of the action, recognize its significance and be aware of the expectations associated with it (Chen *et al.*, 2018). GSM participation can shape an individual's perceptions and opinions (Guo *et al.*, 2021). Tang *et al.* (2021) found that engaging in GSM contributes positively to individuals' motivation to adopt protective measures against cyber scams via perceived severity, perceived vulnerability, self-efficacy and response efficacy. Based on these arguments, the following is proposed:

H5. Government social media has a positive impact on information protection motivation.

2.3.4 Organizational policy compliance, cybersecurity awareness and employee protective behavior On the basis of the PMT framework, it can be inferred that individuals who possess greater awareness of cyberthreats are more likely to actively seek out information on securing their devices (Klein and Zwilling, 2023). This heightened awareness is likely to increase compliance with organizational policy. Organizational policy compliance is widely believed to significantly influence employees' behaviors and enhance an organization's information security level (Chen *etal.*, 2018). A cybersecurity policy with an understandable rationale can influence protective behaviors (D'Arcy et *al.*, 2009; Safa et *al.*, 2015). However, several scholars argue that awareness of cybersecurity policy, not the content of the cybersecurity policy itself, significantly influences computer misuse intentions and abuse behaviors such as modifying, stealing or destroying software and data (Lee *et al.*, 2004; Lee and Larsen, 2009). Indeed, raising employees' awareness of security policies positively contributes to their beliefs about cybersecurity and their behavior in protecting information security (Li et *al.*, 2019). Because previous results are contradictory, in this study, we reinvestigate the relationship between organizational policy compliance and employee protective behavior in the specific context of governmental organizations:

H6. Organizational policy compliance has a positive impact on cybersecurity awareness.

H7. Organizational policy compliance has a positive impact on employee protective behavior.

Figure 1 compiles the hypotheses into the research model.

3. Methodology

3.1 Measurement

All constructs were assessed using a seven-point Likert scale ranging from 1 (strongly disagree) to 7 (strongly agree). The measurement items on the questionnaire were adapted from previous studies with minor or major modifications. The first part of the survey collected demographic information such as gender, age, education level, working tenure and organizational size. The second section included the constructs and their corresponding measurement items. The indicators for organizational policy compliance and perceived severity were adapted from Hina *et al.* (2019). The measures for perceived vulnerability and response efficacy were drawn from previous studies (Hina *et al.*, 2019; Li *et al.*, 2019; Wong *et al.*, 2022). Self-efficacy was measured using items adapted from Hina *et al.* (2019) and Li *et al.* (2022). The GSM items were adapted from Tang *et al.* (2021). Information protection motivation was evaluated using measurement scales from Ma (2022) and Posey *etal.* (2015). The measures of employees' protective behaviors were adapted from Bulgurcu *et al.* (2010) and Wong *etal.* (2022). Table A1 in the Appendix describes the measurement of all variables.

3.2 Data collection

The survey was initially written in English and subsequently translated into Vietnamese to facilitate its distribution to a wider range of participants. A pilot study of 30 respondents was performed to assess the appropriateness of the translation in the Vietnamese context. Based on the results, modifications were made to improve the clarity and readability of the questionnaire. From October 2022 to March 2023, data were collected by distributing the survey to public servants working at governmental organizations. We received invaluable support from local authorities to distribute the survey in their organizations.

The data were collected by applying nonprobability methods, specifically, a stratification approach. According to this approach, questionnaires were sent to 200 public personnel in each region of Ho Chi Minh City and Hanoi Capital. In addition, 150 surveys were disseminated in two adjacent provinces: Dong Nai Province and Binh Duong Province. In total, 700 questionnaires were distributed, and 564 were returned, of which 330 responses were valid.

3.3 Methodology

Partial least squares-structural equation modeling (PLS-SEM) was used to analyze the data and evaluate the research model. PLS-SEM is a variance-based approach that assesses partial model structures by integrating principal component analysis and ordinary least squares regression (Hair *et al.*, 2020). PLS-SEM is widely used in several disciplines, including research on cybersecurity behaviors (Alanazi et *al.*, 2022; Wong et *al.*, 2022). PLS-SEM aligns well with our research objectives for several reasons. First, it can test a theoretical framework from a predictive standpoint. Second, it provides support for the structural model, which is complex and encompasses numerous constructs, indicators, dependent components and model relationships. Finally, it enhances comprehension when exploring extensions of established theories (Hair *etal.*, 2019).

4. Results

4.1 Demographic characteristics

The demographic profile and organizational characteristics of the respondents are shown in Table 1. Among the respondents, 26.67% are men, and 74.0% are women. The majority (71.21%) are 18-35 years old. Over 72% of the participants possess a bachelor's degree or higher, 66.97% have more than five years of working experience and 52.42% work at large organizations with more than 100 employees.

4.2 Common method bias

The methodology used in this study raises the risk of common method bias (CMB) because the questionnaire instructions and social desirability may affect the respondents' answers, leading to shared variation among indicators (Kock, 2015). Full collinearity variance inflation factors (FCVIFs) can effectively detect CMB, even in a model that satisfies the standard criteria for convergent and discriminant validity based on confirmatory factor analysis (Kock, 2015). If all FCVIFs obtained through a full collinearity test are 3.3 or less, then the model is considered free from CMB (Kock, 2015). As shown in Table 3, the FCVIFs for all latent constructs are below the 3.3 threshold, implying that the collected data are unaffected by CMB.

4.3 Validity and reliability

The construct measures' validity and reliability test statistics are presented in Tables 2 and 3. Factor loadings exceeding 0.70 are recommended to ensure acceptable item reliability (Hair et *al.*, 2020). As shown in Table 3, all indicators exhibit factor loadings

Table 1 Characteristics of the respondents

Demographic items	*Frequency (n = 330)*	*%*
Gender		
Female	88	26.67
Male	242	73.33
Age		
18-35 years	235	71.21
36-45 years	73	22.12
Over 45 years	22	6.67
Education level		
High school	90	27.27
Undergraduate	185	56.06
Postgraduate	55	16.67
Working experience		
Less than 3 years	49	14.85
3-5 years	60	18.18
More than 5 years	221	66.97
Organizational size		
Fewer than 50 employees	98	29.70
51-100 employees	59	17.88
More than 100 employees	173	52.42

Source: Created by the authors

exceeding this threshold except RE10, which has a factor loading of 0.662. Thus, RE10 was eliminated from the analysis.

Internal consistency reliability can be assessed using both Cronbach's alpha (a) and composite reliability (CR); values greater than 0.70 are recommended for both reliability measures (Hair *et al.*, 2020). Table 3 shows that all constructs have both a and CR values above 0.70, indicating satisfactory to good reliability.

An average variance extracted (AVE) value of 0.50 or greater signifies that the construct accounts for at least 50% of the variance in its items (Hair *etal.*, 2020). In this study, all AVE values of the constructs are higher than 0.50, implying that the convergent validity test is satisfied.

Finally, discriminant validity was tested by using the heterotrait-monotrait (HTMT) ratio and Fornell-Larcker criterion (Hair *etal.*, 2020). HTMT ratio compares the correlations of an item across constructs to its correlations with the same construct, and an upper boundary of 0.85 or 0.90 (Hair et *al.*, 2019) is suggested to avoid discriminant validity issues. The Fornell-Larcker criterion is fulfilled when a factor's squared AVE exceeds the square root of its inter-construct correlations (Fornell and Larcker, 1981). As shown in Table 4, all constructs meet the requirements for both the HTMT ratio and Fornell-Larcker criterion, implying acceptable levels of discriminant validity.

4.4 Structural model assessment

As there is no standard goodness-of-fit statistic for PLS-SEM, the quality of the model is evaluated based on its capacity to predict the endogenous constructs (Hair et *al.*, 2019). This evaluation is guided by the coefficient of determination *(R^2)* and the effect size *(f^2)* (Hair *etal.*, 2019).

R^2 indicates the collective impact of the exogenous variables on the endogenous variables and ranges from 0 to 1, with 1 indicating absolute predictive accuracy (Hair *etal.*, 2019). R^2 values of 0.75, 0.50 and 0.25 are interpreted as indicating substantial, moderate and weak

Table 2 Factor analysis with reliability and validity statistics

Constructs (> 0.5)	*Item no.*	*Loadings (> 0.7) FCVIF(< 3.3)*	*a(> 0.7)*		*CR(> 0.7)*	*AVE*
Employee protective behavior (EPB)	EPB1	0.918	0.915	0.917	0.855	2.880
	EPB2	0.936				
	EPB3	0.920				
Government social media (GSM)	GSM1	0.911	0.899	0.899	0.831	3.255
	GSM2	0.919				
	GSM3	0.905				
Information protection motivation (IPM)	IPM1	0.895	0.947	0.947	0.825	1.106
	IPM2	0.892				
	IPM3	0.903				
	IPM4	0.932				
	IPM5	0.920				
Organizational policy compliance (OPC)	OPC1	0.893	0.926	0.927	0.818	2.182
	OPC2	0.933				
	OPC3	0.872				
	OPC4	0.919				
Cybersecurity awareness (second-order	*variable)*					
Perceived severity (PS)	PS1	0.845	0.924	0.926	0.686	1.838
	PS2	0.818				
	PS3	0.802				
	PS4	0.847				
	PS5	0.811				
	PS6	0.825				
	PS7	0.850				
Perceived vulnerability (PV)	PV1	0.796	0.903	0.906	0.631	1.484
	PV2	0.792				
	PV3	0.815				
	PV4	0.776				
	PV5	0.785				
	PV6	0.782				
	PV7	0.814				
Response efficacy (RE)	RE1	0.873	0.938	0.942	0.670	2.516
	RE2	0.865				
	RE3	0.841				
	RE4	0.828				
	RE5	0.795				
	RE6	0.805				

	RE7	0.801				
	RE8	0.841				
	RE9	0.705				
	RE10	Eliminated				
Self-efficacy (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				

Source: Created by the authors

predictive accuracy, respectively (Hair *etal.,* 2019). In our model, the *R2* values of the three endogenous variables - cybersecurity awareness, information protection motivation and employee protective behavior - are 0.614, 0.654 and 0.682, respectively. These values indicate moderate to substantial predictive accuracy.

f^2 is used to evaluate the effect of removing a specific predictor construct on the R^2 of an endogenous variable (Hair *et al.,* 2019). f^2 values of 0.02, 0.15 and 0.35 indicate small, medium and large effect sizes, respectively. The relationships investigated in this study have

Table 3 HTMT ratio and Fornell-Larcker criterion

Constructs	*EPB*	*OPC*	*GMS*	*IPM*	*PS*	*PV*	*RE*	*SE*
HTMT ratio								
Employee protective behavior (EPB) Organizational policy compliance (OPC)	0.745							
Government social media (GSM)	0.855	0.849						
Information protection motivation (IPM)	0.864	0.761	0.799					
Perceived severity (PS)	0.667	0.594	0.601	0.728				
Perceived vulnerability (PV)	0.457	0.417	0.394	0.473	0.592			
Response efficacy (RE)	0.743	0.820	0.760	0.827	0.747	0.514		
Self-efficacy (SE)	0.724	0.684	0.719	0.688	0.531	0.488	0.813	
Fornell-Larcker criterion								
Employee protective behavior (EPB)	0.925							
Organizational policy compliance (OPC)	0.685	0.904						
Government social media (GSM)	0.775	0.773	0.912					
Information protection motivation (IPM)	0.805	0.713	0.737	0.908				
Perceived severity (PS)	0.615	0.550	0.549	0.682	0.828			
Perceived vulnerability (PV)	0.420	0.387	0.359	0.440	0.540	0.794		
Response efficacy (RE)	0.695	0.766	0.703	0.782	0.691	0.472	0.818	
Self-efficacy (SE)	0.671	0.640	0.663	0.650	0.501	0.457	0.775	0.863

Source: Created by the authors

Table 4 Hypothesis testing results

	Hypothesis	*b*	*t-value*	*p-value*	*Remarks*
H1	CSA ! EPB	0.188	2.335	0.020	Supported
H2	CSA ! IPM	0.493	7.161	0.000	Supported
H3	GSM ! CSA	0.359	4.102	0.000	Supported
H4	GSM ! IPM	0.379	4.918	0.000	Supported
H5	IPM ! EPB	0.555	6.025	0.000	Supported
H6	OPC ! CSA	0.476	6.023	0.000	Supported
H7	OPC ! EPB	0.148	1.592	0.111	Not supported

Notes: CSA = Cybersecurity awareness; EPB = Employee protective behavior; IPM = Information protection motivation; GSM = Government social media; OPC = Organizational policy compliance

Source: Created by the authors

medium or large effect sizes, excluding the relationships between cybersecurity awareness and employee protective behavior and between organizational policy compliance and employee protective behavior, which have f^2 values of 0.031 and 0.028, respectively.

4.5 Hypothesis testing

The hypothesis testing results are presented in Table 4. A hypothesis is accepted when the p-value is < 0.05 or the corresponding t-value is >1.96; otherwise, it is rejected. All hypotheses are supported, except *H7*. Cybersecurity awareness positively affects information protection motivation and employee protective behavior *(b* = 0.501, *b* = 0.175 and *p* < 0.05), supporting *H1* and *H2*. GSM positively influences cybersecurity awareness and information protection motivation (*b* = 0.375, *b* = 0.365 and p < 0.05); thus, *H3*and *H4* are accepted. The correlation between information protection motivation and employee protective behavior is significantly positive (*b* = 0.562 and p = 0.000), supporting *H5*. Organizational policy compliance strongly enhances cybersecurity awareness (*b* = 448 and p < 0.05), confirming *H6*. However, H7, which posits a positive impact of organizational policy compliance on employee protective behavior, is rejected because its p-value of 0.109 and t-value of 1.604 do not meet the recommended thresholds.

4.6 Mediating effects

Indirect effects were evaluated to assess three potential mediating relationships: information protection motivation as a mediator of the relationship between cybersecurity awareness and employee protective behavior; cybersecurity awareness as a mediator of the relationship between GSM and information protection motivation; and cybersecurity awareness as a mediator of the relationship between organizational policy compliance and employee protective behavior. As shown in Table 5, the direct and indirect effects in the first two relationships are significantly positive (*b* > 0 and *p* < 0.05). For the third relationship, the direct effect is not supported, but the indirect effect is significantly positive (*b* = 0.079 and p = 0.05). For the first two relationships, the indirect and direct effects have the same direction, indicating complementary mediation. By contrast, cybersecurity awareness fully mediates the relationship between organizational policy compliance and employee protective behavior.

4.7 Discussion

This study examines how GSM and organizational policy compliance affect employees' cybersecurity awareness, motivation and behaviors. Our findings substantiate six of the seven proposed hypotheses. Specifically, cybersecurity awareness is found to positively impact information protection motivation and to directly positively influence employee protective behavior, consistent with a previous study (Tang *etal.*, 2021). Wong *etal.* (2022) also observed that cybersecurity awareness significantly improves employees' proficiency in handling cybersecurity tasks in response to perceived threats, and awareness has been shown to directly impact cyber-misuse prevention and cybersecurity policy compliance (Bulgurcu *et al.*, 2010; D'Arcy *et al.*, 2009). In addition, a significant positive correlation is observed between information protection motivation and employee protective behavior. This result aligns with the research of Ma (2022), who concluded that protection motivation is a robust predictor of behavior. Information protection motivation also partially mediates the relationship between cybersecurity awareness and employee protective behavior.

GSM has a positive influence on cybersecurity awareness, consistent with prior suggestions that GSM is the primary source of crisis-related information (Intravia *etal.*, 2017; Shah *etal.*, 2020; Tang *etal.*, 2021). Active engagement with GSM not only leads individuals to believe that cyberattack-related media events can affect them but also equips them with the knowledge and preparedness needed to respond effectively, thereby enhancing cybersecurity awareness. Cybersecurity awareness also partially mediates the relationship between GSM and information protection motivation. This observation aligns with the

findings of Tang *et al.* (2021), who claim that social media information consumption motivates users to take preventive actions. By demonstrating a direct impact of GSM on information protection motivation, this study provides a novel perspective, as prior research has predominantly investigated the influence of GSM on motivation and behaviors by measuring variables such as fear of victimization.

Table 5 Mediating effects

	Hypothesis	*Type*	*b*	*t-value*	*p-value*	*Remarks*
H1	CSA ! EPB	Direct	0.188	2.335	0.020	Supported
	CSA ! IPM ! EPB	Indirect	0.274	4.947	0.000	Complementary (partial mediation)
H4	GSM ! IPM	Direct	0.379	4.918	0.000	Supported
	GSM ! CSA ! IPM	Indirect	0.177	3.487	0.000	Complementary (partial mediation)
H7	OPC ! EPB	Direct	0.148	1.592	0.111	Not supported
	OPC ! CSA ! EPB	Indirect	0.068	1.806	0.071	Indirect only (full mediation)

Source: Created by the authors

Last but not least, organizational policy compliance substantially boosts cybersecurity awareness. However, there is no direct impact of organizational policy compliance on employee protective behavior; instead, this relationship is fully mediated by cybersecurity awareness. Hina *et al.* (2019) suggested that to enhance security behavior and actions, organizations must go beyond distributing organizational cybersecurity policies and ensuring familiarity with their content; employees must fully perceive the severity of a security breach and the organization's vulnerability to it. The mediating role of cybersecurity awareness underscores the importance of not only formulating a cybersecurity policy but also implementing processes to disseminate and instill it in the minds of employees to enhance protective behaviors.

5. Implications and conclusion

5.1 Theoretical contributions

First, the present study provides a comprehensive analysis of the literature on cybersecurity awareness, motivation and behavior. This study extends the PMT and cultivation theory by incorporating employee protective behavior as a crucial factor and examining the connection between this concept and information protection motivation. Assessing real actions is an essential component of cybersecurity research, as the main objective is to enhance security practices rather than just intentions. This study demonstrates that cybersecurity awareness and information protection motivation both significantly influence employee protective behavior.

Second, this study integrates four cognitive factors (perceived severity, perceived vulnerability, self-efficacy and response efficacy) to create the second-order construct of cybersecurity awareness. This multidimensional construct reflects the complexity of cybersecurity awareness while simplifying the model and reducing the number of hypotheses, allowing us to focus on what truly matters and uncover meaningful insights.

Third, our conceptual framework incorporates the effects of cultivation through GSM to investigate the antecedents of cybersecurity awareness. The literature primarily focuses on understanding why individuals engage with GSM during crises and on categorizing the emergency messaging strategies used by GSM (Tang *et al.*, 2021). These studies neglect the impact of GSM on individuals' awareness of and motivation toward perennially urgent issues such as cybersecurity policy, particularly when individuals enthusiastically engage with cybersecurity content shared on GSM. Our results confirm that GSM positively affects both cybersecurity awareness and information protection motivation.

Finally, there is no consensus in the literature on the effectiveness of cybersecurity policies, particularly their impact on protective behaviors. Therefore, we investigate the direct influence of organizational cybersecurity compliance on protective behavior and its indirect effect through cybersecurity awareness. Our findings indicate that organizational policy

compliance does not have a direct impact on employee protective behavior; instead, its influence is mediated by cybersecurity awareness.

5.2 Practical implications

This research provides a robust foundation for senior management of public organizations to formulate strategic solutions addressing deficiencies in the governance, utilization and operation of computer systems and networks. Empirical studies have predominantly focused on the private sector, and the applicability and transferability of the findings to public organizations remain unclear. Public organizations are progressively embracing digitalization to enhance the flow and storage of operational data. However, current organizational policies for managing and using computer systems are insufficient to support these digitalization efforts, increasing the risk of information insecurity.

Organizational policy noncompliance occurs in the public sector when public officials, despite having a fundamental understanding of cybersecurity, fail to comply with agency standards. Cyberspace policy noncompliance, such as using unverified data from USB drives or accessing online resources without permission, can compromise network security and threaten privileged government computer system data. By adopting robust international standards-based laws, government organizations can strengthen their cyber defenses and encourage employee compliance. This will safeguard vital assets and boost government credibility.

Organizational policy compliance also affects employees' cybersecurity behavior. This study finds that following the law indirectly increases employees' cybersecurity awareness and willingness to take precautions. Organizations must go beyond policies to improve compliance and cybersecurity. They should invest more in training, cybersecurity newsletters and alarm alerts. These activities are essential for effective policy dissemination and employee comprehension of cybersecurity threats and best practices. Organizations can foster a cybersecurity-savvy and regulatory-compliant culture by engaging employees through many channels, which will improve the overall security stance of the organization.

Considering the significant impacts of GSM on cybersecurity awareness and information protection motivation, government organizations should maintain an active role in disseminating cybersecurity information quickly and concisely through their GSM channels. Specifically, government-operated social media platforms play a significant role in enhancing recent governmental endeavors focused on advancing cybersecurity. Through these platforms, governments can swiftly disseminate crucial information regarding emerging cyber threats, best practices for online safety and updates on cybersecurity policies and regulations. Similarly, governments may effectively use the extensive reach and convenient accessibility of social media platforms to interact directly with citizens, thereby cultivating a collective feeling of accountability and empowerment in the protection of digital assets. Furthermore, social media platforms play a crucial role in facilitating instantaneous communication, allowing governments to rapidly disseminate alerts and updates. This, in turn, aids individuals in being watchful against the ever-changing landscape of cyber dangers. Moreover, these platforms offer opportunities for interactive communication, enabling individuals to seek advice, exchange knowledge and engage in cooperative endeavors aimed at enhancing cybersecurity resilience. GSM serves to both expand the scope of cybersecurity awareness programs and cultivate a more knowledgeable and involved populace, which is essential for improving the overall cybersecurity posture.

5.3 Conclusions

This study uses a quantitative survey and PLS-SEM to examines the influence of GSM and organizational policy compliance on behavioral aspects of cybersecurity. Additionally, this study extends the PMT and cultivation theory by introducing employee protective behavior as a dependent variable and constructing a conceptual framework that integrates cultivation effects with GSM. The results offer novel insights into the complex interplay among GSM, cybersecurity awareness, information protection motivation and employee protective behavior. Specifically, cybersecurity awareness positively impacts both information protection motivation and employee protective behavior. Moreover, GSM positively affects cybersecurity awareness and information protection motivation, with cybersecurity playing a partial mediating role in the relationship between GSM and information protection motivation. Furthermore,

a significant positive correlation exists between information protection motivation and employee protective behavior, and information protection motivation partially mediates the relationship between cybersecurity awareness and employee protective behavior. Finally, organizational policy compliance significantly enhances cybersecurity awareness. However, organizational policy compliance does not directly impact employee protective behavior; instead, this relationship is fully mediated by cybersecurity awareness.

5.4 Limitations and future studies

While this study provides new insights into theory and practice, it has certain limitations. First, measuring employee protective behavior using a self-report quantitative questionnaire may lack validity. Self-reports may not be reliable predictors of employees' actual behavior, as their perceptions of security behavior might not align with their real security practices. Longitudinal research would enable more accurate records of actual behavior records but require more time and effort. Second, control variables such as gender, job title and organizational size are not considered, and it would be valuable to explore how these factors influence the established relationships. Third, investigating additional variables at the individual, organizational and social levels would provide a more comprehensive view of the antecedents of employees' protective behaviors.

References

Alanazi, M., Freeman, M. and Tootell, H. (2022), "Exploring the factors that influence the cybersecurity behaviors of young adults", *Computers in Human Behavior*, Vol. 136, pp. 1-14, doi: 10.1016/j.chb.2022.107376.

AlKalbani, A., Deng, H., Kam, B. and Zhang, X. (2017), "Information security compliance in organizations: an institutional perspective", *Data and Information Management*, Vol. 1 No. 2, pp. 104-114, doi: 10.1515/ dim-2017-0006.

Alshaikh, M., Maynard, S.B. and Ahmad, A. (2021), "Applying social marketing to evaluate current security education training and awareness programs in organisations", *Computers & Security*, Vol. 100, pp. 1-19, doi: 10.1016/j.cose.2020.102090.

Bauer, S., Bernroider, E.W.N. and Chudzikowski, K. (2017), "Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks", *Computers & Security*, Vol. 68, pp. 145-159, doi: 10.1016/j.cose.2017.04.009.

Boss, S., Galletta, D., Lowry, P.B. and Moody, G.D. (2015), "What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective behaviors in users", *MIS Quarterly*, Vol. 39 No. 4, pp. 837-864, doi: 10.25300/MISQ/2015/39.4.5.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, Vol. 34 No. 3, pp. 523-548.

Chen, X., Chen, L. and Wu, D. (2018), "Factors that influence employees' security policy compliance: an awareness-motivation-capability perspective", *Journal of Computer Information Systems*, Vol. 58 No. 4, pp. 312-324, doi: 10.1080/08874417.2016.1258679.

Chowdhury, N.H., Adam, M.T.P. and Skinner, G. (2019), "The impact of time pressure on cybersecurity behaviour: a systematic literature review", *Behaviour & Information Technology*, Vol. 38 No. 12, pp. 1290-1308, doi: 10.1080/0144929X.2019.1583769.

Corallo, A., Lazoi, M., Lezzi, M. and Luperto, A. (2022), "Cybersecurity awareness in the context of the industrial internet of things: a systematic literature review", *Computers in Industry*, Vol. 137, pp. 1-16, doi: 10.1016/j.compind.202Z103e14.

D'Arcy, J., Hovav, A. and Galletta, D. (2009), "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach", *Information Systems Research*, Vol. 20 No. 1, pp. 79-98, doi: 10.1287/isre.1070.0160.

Del Vecchio, P., Mele, G., Passiante, G., Vrontis, D. and Fanuli, C. (2020), "Detecting customers knowledge from social media big data: toward an integrated methodological framework based on netnography and business analytics", *Journal of Knowledge Management*, Vol. 24 No. 4, pp. 799-821, doi: 10.1108/JKM-11-2019-0637.

Farooq, A., Laato, S. and Najmul Islam, A.K.M. (2020), "Impact of online information on self-isolation intention during the COVID-19 pandemic: cross-sectional study", *Journal of Medical Internet Research*, Vol. 22 No. 5, doi: 10.2196/19128.

Floyd, D., Prentice-Dunn, S. and Rogers, R. (2000), "A Meta-Analysis of research on protection motivation theory", *Journal of Applied Social Psychology*, Vol. 30 No. 2, pp. 407-429, doi: 10.1111/j.1559-1816.2000. tb02323.x.

Fornell, C. and Larcker, D.F. (1981), "Structural equation models with unobservable variables and measurement error: algebra and statistics", *Journal of Marketing Research*, Vol. 18 No. 3, pp. 382-388, doi: 10.2307/3150980.

Fosch-Villaronga, E. and Mahler, T. (2021), "Cybersecurity, safety and robots: strengthening the link between cybersecurity and safety in the context of care robots", *Computer Law & Security Review*, Vol. 41, pp. 1-13, doi: 10.1016/j.clsr.2021.105528.

Gerbner, G. and Gross, L. (1976), "Living with television: the violence profile", *Journal of Communication*, Vol. 26 No. 2, pp. 172-199, doi:10.1111/j.1460-2466.1976.tb01397.x.

Guo, J., Liu, N., Wu, Y. and Zhang, C. (2021), "Why do citizens participate on government social media accounts during crises? A civic voluntarism perspective", *Information & Management*, Vol. 58 No. 1, pp. 1-12, doi: 10.1016/j.im.2020.103286.

Hair, J.F., Jr., Howard, M.C. and Nitzl, C. (2020), "Assessing measurement model quality in PLS-SEM using confirmatory composite analysis", *Journal of Business Research*, Vol. 109, pp. 101-110, doi: 10.1016/j.jbusres.2019.11.069.

Hair, J.F., Risher, J.J., Sarstedt, M. and Ringle, C.M. (2019), "When to use and how to report the results of PLS-SEM", *European Business Review*, Vol. 31 No. 1, pp. 2-24, doi: 10.1108/EBR-11- 2018-0203.

Hanus, B., Windsor, J.C. and Wu, Y. (2018), "Definition and multidimensionality of security awareness: close encounters of the second order", *ACM SIGMIS DATABASE: The Database for Advances in Information Systems*, Vol. 49 No. 1, pp. 103-133

Hasan, S., Ali, M., Kurnia, S. and Thurasamy, R. (2021), "Evaluating the cyber security readiness of organizations and its influence on performance", *Journal of Information Security and Applications*, Vol. 58, pp. 1-16, doi: 10.1016/j.jisa.2020.102726.

Hermann, E., Eisend, M. and Bayon, T. (2020), "Facebook and the cultivation of ethnic diversity perceptions and attitudes", Internet Research, Vol. 30 No. 4, pp. 1123-1141, doi: 10.1108/INTR-10-2019- 0423.

Hina, S. and Dominic, P.D.D. (2020), "Information security policies' compliance: a perspective for higher education institutions", *Journal of Computer Information Systems, Online First*, Vol. 60 No. 3, doi: 10.1080/ 08874417.2018.1432996.

Hina, S., Panneer Selvam, D.D.D. and Lowry, P.B. (2019), "Institutional governance and protection motivation: theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world", *Computers & Security*, Vol. 87, pp. 1-15, doi: 10.1016/j. cose.2019.101594.

Ifinedo, P. (2012), "Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory", *Computers & Security*, Vol. 31 No. 1, pp. 83-95, doi: 10.1016/j.cose.2011.10.007.

Intravia, J., Wolff, K.T., Paez, R. and Gibbs, B.R. (2017), "Investigating the relationship between social media consumption and fear of crime: a partial analysis of mostly young adults", *Computers in Human Behavior*, Vol. 77, pp. 158-168, doi: 10.1016/j.chb.2017.08.047.

Islm, T., Meng, H., Pitafi, A.H., Ullah Zafar, A., Sheikh, Z., Shujaat Mubarik, M. and Liang, X. (2021), "Why DO citizens engage in government social media accounts during COVID-19 pandemic? A comparative study", *Telematics and Informatics*, Vol. 62, p. 101619, doi: 10.1016/j.tele.2021.101619.

Jain, N. and Raman, T.V. (2023), "The interplay of perceived risk, perceive benefit and generation cohort in digital finance adoption", *EuroMed Journal of Business*, Vol. 18 No. 3, pp. 359-379, doi: 10.1108/EMJB- 09-2021-0132.

Klein, G. and Zwilling, M. (2023), "The weakest link: employee Cyber-Defense behaviors while working from home", *Journal of Computer Information Systems, pp*, Vol. 64 No. 3, pp. 1-15, doi: 10.1080/ 08874417.2023.2221200.

Kock, N. (2015), "Common method bias in PLS-SEM: a full collinearity assessment approach", *International Journal of e-Collaboration*, Vol. 11 No. 4, pp. 1-10, doi: 10.4018/ijec.2015100101.

Lee, Y. and Larsen, K.R. (2009), "Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 177-187, doi: 10.1057/ejis.2009.11.

Lee, S.M., Lee, S.G. and Yoo, S. (2004), "An integrative model of computer abuse based on social control and general deterrence theories", *Information & Management*, Vol. 41 No. 6, pp. 707-718, doi: 10.1016/j. im.2003.08.008.

Li, L., Xu, L. and He, W. (2022), "The effects of antecedents and mediating factors on cybersecurity protection behavior", *Computers in Human Behavior Reports*, Vol. 5, pp. 1-14, doi: 10.1016/j.chbr.2021.100165.

Li, L., He, W., Xu, L., Ash, I., Anwar, M. and Yuan, X. (2019), "Investigating the impact of cybersecurity policy awareness on employees ' cybersecurity behavior", *International Journal of Information Management*, Vol. 45, pp. 13-24, doi: 10.1016/j.ijinfomgt.2018.10.017.

Lu, Y. and Xu, L.D. (2019), "Internet of things (IoT) cybersecurity research: a review of current research topics", *IEEE Internet of Things Journal*, Vol. 6 No. 2, pp. 2103-2115, doi: 10.1109/ JIOT.2018.2869847.

Ma, X. (2022), "Is professionals' information security behaviors in Chinese IT organizations for information security protection", *Information Processing & Management*, Vol. 59 No. 1, doi: 10.1016/j. ipm.2021.102744

Maddux, J.E. and Rogers, R.W. (1983), "Protection motivation and Self-Efficacy: a revised theory of fear appeals and attitude change", *Journal of Experimental Social Psychology*, Vol. 19 No. 5, pp. 469-479, doi: 10.1016/0022-1031 (83)90023-9.

Martens, M., De Wolf, R. and De Marez, L. (2019), "Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general", *Computers in Human Behavior*, Vol. 92, pp. 139-150, doi: 10.1016/j.chb.2018.11.002.

Ou, C.X., Zhang, X., Angelopoulos, S., Davison, R.M. and Janse, N. (2022), "Security breaches and organization response strategy: exploring consumers' threat and coping appraisals", *International Journal of Information Management*, Vol. 65, pp. 1-17, doi: 10.1016/j.ijinfomgt.2022.102498.

Posey, C., Roberts, T.L. and Lowry, P.B. (2015), "The impact of organizational commitment on insiders motivation to protect organizational information assets", *Journal of Management Information Systems*, Vol. 32 No. 4, pp. 179-214, doi: 10.1080/07421222.2015.1138374.

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A. and Herawan, T. (2015), "Information security conscious care behaviour formation in organizations", *Computers & Security*, Vol. 53, pp. 65-78, doi: 10.1016/j.cose.2015.05.012.

Shah, Z., Chu, J., Ghani, U., Qaisar, S. and Hassan, Z. (2020), "Media and altruistic behaviors: the mediating role of fear of victimization in cultivation theory perspective", *International Journal of Disaster Risk Reduction*, Vol. 42, pp. 1-8, doi: 10.1016/j.ijdrr.2019.101336.

Shaw, R.S., Chen, C.C., Harris, A.L. and Huang, H.-J. (2009), "The impact of information richness on information security awareness training effectiveness", *Computers & Education*, Vol. 52 No. 1, pp. 92-100, doi: 10.1016/j.compedu.2008.06.011.

Tang, Z., Miller, A.S., Zhou, Z. and Warkentin, M. (2021), "Does government social media promote users' information security behavior towards COVID-19 scams? Cultivation effects and protective motivations", *Government Information Quarterly*, Vol. 38 No. 2, pp. 1-11, doi: 10.1016/j.giq.2021.101572.

Tu, Z., Turel, O., Yuan, Y. and Archer, N. (2015), "Learning to cope with information security risks regarding mobile device loss or theft: an empirical examination", *Information and Management*, Vol. 52 No. 4, pp. 506-517, doi: 10.1016/j.im.2015.03.002.

van Bavel, R., Rodriguez-Priego, N., Vila, J. and Briggs, P. (2019), "Using protection motivation theory in the design of nudges to improve online security behavior", *International Journal of Human-Computer Studies,VoL* 123, pp. 29-39, doi: 10.1016/j.ijhcs.2018.11.003.

Vance, A., Siponen, M. and Pahnila, S. (2012), "Motivating is security compliance: insights from habit and protection motivation theory", *Information & Management*, Vol. 49 Nos 3/4, pp. 190-198, doi: 10.1016/j. im.2012.04.002.

Vrhovec, S. and Mihelic, A. (2021), "Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation", *Computers & Security*, Vol. 106, pp. 1-22, doi: 10.1016/j.cose.2021.102309.

Vrontis, D., Makrides, A., Christofi, M. and Thrassou, A. (2021), "Social media influencer marketing: a systematic review, integrative framework and future research agenda", *International Journal of Consumer Studies*, Vol. 45 No. 4, pp. 617-644, doi: 10.1111/ijcs.12647.

Wong, L.W., Lee, V.H., Tan, G.W.H., Ooi, K.B. and Sohal, A. (2022), "The role of cybersecurity and policy awareness in shifting employee compliance attitudes: building supply chain capabilities", *International Journal of Information Management*, Vol. 66, pp. 1-15, doi: 10.1016/j.ijinfomgt.2022.102520.

Wu, D. (2020), "Empirical study of knowledge withholding in cyberspace: integrating protection motivation theory and theory of reasoned behavior", *Computers in Human Behavior*, Vol. 105, pp. 1-14, doi: 10.1016/j.chb.2019.106229.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F. and Basim, H.N. (2022), "Cyber security awareness, knowledge and behavior: a comparative study", *Journal of Computer Information Systems*, Vol. 62 No. 1,pp.82-97,doi: 10.1080/088744V.2020.1712269.

Author affiliations

Dien Van Tran is based at the Center For Public Administration, International University VNUHCM, Ho Chi Minh City, Vietnam.

Phuong Van Nguyen is based at the Center For Public Administration, International University VNUHCM, Ho Chi Minh City, Vietnam and Vietnam National University, Ho Chi Minh City, Vietnam.

Demetris Vrontis is based at the Faculty and Research, University of Nicosia, Nicosia, Cyprus; SP Jain School of Global Management, Dubai Campus, Dubai, United Arab Emirates and Department of Management Studies, Adnan Kassar School of Business, Lebanese American University, Beirut, Lebanon.

Sam Thi Ngoc Nguyen is based at The School of Business, International University, Vietnam National University-HCMC, Ho Chi Minh City, Vietnam.

Phuong Uyen Dinh is based at the Office of Administration, Ho Chi Minh City Open University, Ho Chi Minh City, Vietnam.

Appendix

Table A1 Measurement items

Construct (source)	*Code*	*Measurement items*	*Modifications*
Organizational policy compliance (Hina *etal.*, 2019)	OPC1	My organization has established rules of behavior for computer use to comply with governmental regulations	Major modification
	OPC2	My organization has specific guidelines for computer use to comply with governmental regulations	Major modification
	OPC3	My organization has a policy that forbids employees from accessing certain online websites when their computers contain confidential documents to comply with governmental regulations	Major modification
	OPC4	My organization has defined code(s) of conduct explaining the do's and don'ts of information security to comply with governmental regulations	Major modification
Perceived severity (Hina *etal,* 2019)	PS1	Protecting my organization's information is important	Minor modification
	PS2	At work, having my confidential information accessed without my consent or knowledge can be a serious problem for me	No change
	PS3	I understand that having someone successfully breach or damage my information resources at work is very dangerous	No change
	PS4	Loss of data because of hackers is a serious problem for me	Major modification
	PS5	Organizing staff training will be a critical first step to ensure information security	Major modification
	PS6	Risks can be reduced as employees become more aware of the threats and consequences stemming from their negligence	Major modification
	PS7	Through education, the provision of sufficient data and supporting information helps increase employees' cybersecurity awareness	Major modification
Perceived vulnerability (Hina *etal,* 2019; Li *etal.*, 2019; Wong *etal.*, 2022)	PV1	I knowthat my organization could be vulnerable to security breaches if I do not adhere to its Information Security Policies	No change
	PV2	I may fall victim to a malicious attack if I fail to comply with my organization's Information Security Policies	No change
	PV3	In terms of information security risks at work, my computing resources can be vulnerable	No change
	PV4	I believe that every individual who is conscious and makes efforts to protect the organization’s information will reduce the risk of illegal access	Major modification
	PV5	Organizations should invest in using modern cybersecurity technologies	Major modification
	PV6	Organizations need to inform employees about potential	Major modification

		cybersecurity threats regularly	
	PV7	It is likely that a potential information security violation will occur to my organization's information systems	Major modification
Self-efficacy (Hina *etal.*, 2019; Li etal., 2022)	SE1	I believe that I have the necessary skills to protect myself from information security violations	No change
	SE2	I believe that I have developed the capability to prevent people from getting my confidential information	No change
	SE3	I enable security measures (firewall, antivirus, etc.) on my work computing resources	No change
	SE4	I believe that protecting myself from information security violations is within my control	Major modification
	SE5	I feel confident in setting the Web browser to different security levels	No change
	SE6	I feel confident in handling virus-infected files	No change
	SE7	I feel confident in getting rid of spyware and malware from my computer	No change
Response efficacy (Hina *etal.*, 2019; Li *etal.*, 2019; Wong *etal*, 2022)	RE1	In my organization, efforts to ensure the safety of my confidential information are effective	No change
	RE2	In my organization, the available security measures to protect my work information from security violations are effective	No change
	RE3	The preventive measures available to me at my organization to deal with malicious content are effective	No change
	RE4	Security measures at my organization prevent hackers from gaining access to sensitive personal or educational information	No change

(*continued*)

Table A1

Construct (source)	*Code*	*Measurement items*	*Modifications*
	RE5	Complying with the information security policies in my organization will keep security breaches down	No change
	RE6	If I comply with information security policies, then the chance of information security breaches occurring will be reduced	No change
	RE7	Careful compliance with information security policies helps to avoid security problems	No change
	RE8	Organizations can improve information security by showing their employees how security negligence can impact the security posture of an organization	Major modification
	RE9	Organizations should have a General Data Protection Regulation	Minor modification

	RE10	Organizations should upgrade antivirus and firewall software	Minor modification
Government social media (Tang eta/., 2021)	GSM 1	I always read and listen to cybersecurity recommendations posted by the GSM	Major modification
	GSM 2	I always share cybersecurity recommendations posted by the GSM	Major modification
	GSM 3	I always communicate cybersecurity recommendations posted by the GSM	Major modification
Information protection motivation (Ma, 2022; Posey *eta/.*, 2015)	IPM1	I intend to protect my organization from its information security	No change
	IPM2	threats My organization's success level in preventing information security threats is very high	Major modification
	IPM3	I am always willing to engage in activities that protect my organization's information systems from security threats	Major modification
	IPM4	I always expend effort to protect my organization from its information security threats	Major modification
	IPM5	I intend to try my best to prevent information security threats from happening in my organization	No change
Employee protective behavior (Li *eta/.*, 2019)	EPB1	I keep the anti-virus software on my computer up-to-date	No change
	EPB2	I watch for unusual computer behaviors/responses (e.g. computer slowing down or freezing up, pop-up windows, etc.)	No change
	EPB3	I am always concerned about any malware that is reported through media channels	Major modification

Source: Created by the authors

Exploring the impact of social capital on business performance: The role of dynamic capabilities, open innovation and government support

Dien Van Tran, Phuong Van Nguyen *, Nhi Tran Thao Dinh, Thang Nam Huynh, Khanh Van Ma

Center for Public Administration, International University, Vietnam National University-Ho Chi Minh City, Ho Chi Minh, Viet Nam

ABSTRACT

Keywords: Social capital (SC), Open innovation (OI), Business performance. Dynamic capabilities (DC), Government support (GS)

This study examines the relationships between social capital (encompassing structural, cognitive, and relational dimensions), dynamic capabilities, open innovation (both inbound and outbound), government support, and business performance in Vietnam. Using a quantitative approach, data were collected from 289 respondents and analyzed using Partial Least Squares Structural Equation Modeling. The findings show that social capital posi-tively influences both dynamic capabilities and open innovation. While dynamic capabilities have a significant impact on business performance, open innovation enhances government support but does not directly affect business performance. Additionally, dynamic capabilities mediate the relationship between social capital and business performance, and government support partially mediates the relationship between open innovation and business performance. These results underscore the importance of government support and dynamic capabilities in leveraging social capital for enhanced business performance, while also highlighting the need for further investigation into the direct impacts of open innovation on performance.

1. Introduction

Government support is a fundamental driver of business growth and innovation in emerging markets like Vietnam, where public policies address market imperfections and provide essential resources for firms to enhance their competitive edge. Vietnamese businesses, especially in sectors such as manufacturing and technology, benefit significantly from government subsidies, tax incentives, and infrastructure investments OECD (2023). However, the extent to which firms can fully leverage this support is not solely determined by government initiatives. Instead, the effectiveness of government support depends largely on the firms' ability to utilize critical internal and external capabilities. Therefore, this study investigates the combined roles of social capital (SC), dynamic capabilities (DC), and open innovation (OI) in determining how gov-ernment support impacts business performance in Vietnam.

Social capital is crucial in Vietnam's emerging economy, where formal institutions may be underdeveloped, and business operations often rely on informal networks and trust-based relationships. SC en-hances collaboration, enables firms to navigate complex regulatory en-vironments, and facilitates access to government support. More importantly, it fosters the development of relational networks that improve knowledge sharing and resource allocation (Mitchelmore and Rowley, 2010). SC also helps firms engage in open innovation and attract government support. As a result, SC is indispensable for busi-nesses aiming to improve performance through better resource alloca-tion, knowledge sharing, and relationship-building, whether in formal or informal settings. In markets where formal institutions are underde-veloped, SC becomes even more significant, making it a critical deter-minant of business success (Annamalah et al., 2023; Nahapiet and Ghoshal, 1998). Furthermore, SC extends beyond relational advantages, directly influencing firms' ability to engage in dynamic capabilities and open innovation.

In parallel, dynamic capabilities, in turn, are essential for firms operating in industries characterized by rapid technological advance-ments, such as manufacturing and technology. DCs allow firms to reconfigure their resources, integrate external knowledge, and adapt to shifts in market demands. These abilities are critical as Vietnam tran-sitions to an innovation-driven economy (Teece et al., 2016). Moreover, the capacity to develop and utilize DCs is often shaped by the firm's social capital, which supports learning and reconfiguration processes (Teece et al., 1997).

Furthermore, open innovation has become increasingly vital for firms in globalized markets. OI enables firms to leverage both internal and external knowledge, facilitating new product development and expanding their reach into international markets (Cano-Kollmann et al., 2017; Chesbrough and Bogers, 2014; Gassmann et al., 20101. Introduction

Government support is a fundamental driver of business growth and innovation in emerging markets like Vietnam, where public policies address market imperfections and provide essential resources for firms to enhance their competitive edge. Vietnamese businesses, especially in sectors such as manufacturing and technology, benefit significantly from government subsidies, tax incentives, and infrastructure investments OECD (2023). However, the extent to which firms can fully leverage this support is not solely determined by government initiatives. Instead, the effectiveness of government support depends largely on the firms' ability to utilize critical internal and external capabilities. Therefore, this study investigates the combined roles of social capital (SC), dynamic capabilities (DC), and open innovation (OI) in determining how gov-ernment support impacts business performance in Vietnam.

Social capital is crucial in Vietnam's emerging economy, where formal institutions may be underdeveloped, and business operations often rely on informal networks and trust-based relationships. SC en-hances collaboration, enables firms to navigate complex regulatory en-vironments, and facilitates access to government support. More importantly, it fosters the development of relational networks that improve knowledge sharing and resource allocation (Mitchelmore and Rowley, 2010). SC also helps firms engage in open innovation and attract government support. As a result, SC is indispensable for busi-nesses aiming to improve performance through better resource alloca-tion, knowledge sharing, and relationship-building, whether in formal or informal settings. In markets where formal institutions are underde-veloped, SC becomes even more significant, making it a critical deter-minant of business success (Annamalah et al., 2023; Nahapiet and Ghoshal, 1998). Furthermore, SC extends beyond relational advantages, directly influencing firms' ability to engage in dynamic capabilities and open innovation.

In parallel, dynamic capabilities, in turn, are essential for firms operating in industries characterized by rapid technological advance-ments, such as manufacturing and technology. DCs allow firms to reconfigure their resources, integrate external knowledge, and adapt to shifts in market demands. These abilities are critical as Vietnam tran-sitions to an innovation-driven economy (Teece et al., 2016). Moreover, the capacity to develop and utilize DCs is often shaped by the firm's social capital, which supports learning and reconfiguration processes (Teece et al., 1997).

Furthermore, open innovation has become increasingly vital for firms in globalized markets. OI enables firms to leverage both internal and external knowledge, facilitating new product development and expanding their reach into international markets (Cano-Kollmann et al., 2017; Chesbrough and Bogers, 2014; Gassmann et al., 2010

1. Hypothesis development

1.1. Social capital and dynamic capabilities

The connection between DC and supply chains in the context of SMEs (Martinelli et al., 2018). They argue that SMEs must mobilize and reorganize their resources and capabilities to respond effectively to adverse events like COVID-19. This necessitates a flexible and cooper-ative organizational environment, facilitated by strong SC (Pasamar et al., 2015). This highlights the significance of establishing a trust-based internal social environment in cultivating dynamic capa-bilities. Employee trust fosters the seamless exchange of information, which is crucial for reallocating resources and adapting to change (Fainshmidt and Frazier, 2017). An empirical study provides strong evidence to support the idea that a trusting internal environment fosters effective communication and collaboration, which is essential for leveraging DC (Zhang et al., 2023). Based on the arguments presented above, the study extends the social capital to investigate the relationship between SC and DC. Therefore, the first hypothesis is proposed as follows:

H1. SC positively influences DC.

1.2. Social capital on open innovation

Effective OI activities require extensive interaction between part-ners, which helps create trust and respect and lowers opportunistic costs (Ju, 2023). Increased communication frequency during OI helps mini-mize misunderstandings and strengthens mutual understanding and reciprocity (Pylypenko et al., 2023). OI relies on knowledge sharing, enabling firms

and external organizations to learn key tacit knowledge for efficient R&D, extending relationships and accumulating SC (Roh et al., 2021). Furthermore, based on the SCT, SC plays a pivotal role in creative outputs from open innovation networks. It facilitates the flow of information and resources, enhancing a firm's ability to innovate. The presence of robust SC can help firms leverage external knowledge more effectively, leading to improved business performance and innovative outcomes (Al-Omoush et al., 2022). In addition, SC is crucial for creative outputs from OI networks (Annamalah et al., 2023). The ability to ac-quire information and create breakthrough innovations depends on complex human and societal factors (Al-Tit et al., 2022). Based on these discoveries, SC considerably improves the outcomes of OI activities. This leads to the following hypothesis:

H2. SC positively influences OI.

1.3. Dynamic capabilities and business performance

Dynamic capabilities are essential for providing long-term competi-tive advantages in rapidly changing environments (Al-Omoush et al., 2022; Eikelenboom and de Jong, 2019), and they allow businesses to better customize products and services for individual customers (Wang et al., 2015). This adaptability explains how companies can thrive in fast-evolving settings (Teece, 2007). Research has consistently shown a positive link between DC and business performance, highlighting their impact on profitability and organizational dynamism (Mohaghegh et al., 2021; Protogerou et al., 2012). The connection between DC and sus-tainability, encompassing environmental, social, and economic aspects, has also been studied. This includes developing social and entrepre-neurial competencies (Marcus and Anderson, 2006). In sustainability contexts, DC refer to a company's ability to meet evolving stakeholder expectations by modifying functional capabilities for economic, envi-ronmental, and social responsibilities (Mohaghegh et al., 2021). Thus, DC not only enhance a firm's ability to adapt to market changes but also support sustainable business practices, leading to improved firm per-formance (Priyono and Hidayat, 2024). Based on these insights, it can be hypothesized that:

H3. DC positively influence business performance.

1.4. Open innovation and government support

International cooperation activities benefit businesses thanks to the support policies of the Government that allow the acquisition and innovation of new technologies (Jugend et al., 2020) in various forms, including grants, tax incentives, state-sponsored, and direct investments through public venture capital (Fernandez-Pinto et al., 2024; Jugend et al., 2018; Srisathan et al., 2023). Open innovation enhances internal and external knowledge flows, improving the innovation process (Cano-Kollmann et al., 2017; Chesbrough and Bogers, 2014). These forms of support are crucial as they directly and indirectly influence firms' innovation activities by stimulating internal R&D, intellectual capital, and entrepreneurial capital (Cano-Kollmann et al., 2017; Holl and Rama, 2012). Furthermore, the focus on supporting micro, small, and medium enterprises is particularly strong due to their significant contributions to industrial renewal, job creation, export growth, and productivity (Doh and Kim, 2014; Srisathan et al., 2023). Innovation policies are increasingly geared towards supporting networks of in-novators, making GS for innovation more widespread and impactful (Bogers et al., 2018). Given these points, it can be hypothesized that:

H4. OI positively influences GS.

1.5. Government support and business performance

According to the SCT, organizations with strong external linkages to the government, financial institutions, and other businesses might gain access to scarce resources that are beneficial to improved performance (Srisathan et al., 2023) such as financial assistance and technology tools (Razumovskaia et al., 2020). By providing a legal framework and tools for businesses to protect themselves from cyberattacks with government support (Hasan et al., 2021). Funding projects improve the results of technology transfer between professors, strengthening direct and indi-rect compenstae the link between professors and performance (Cheah and Ho, 2020; Mai et al., 2024).

These subsidies not only assist organizations earn more income but also serve to validate their R&D projects, promoting additional collab-orations with academic institutions and industry partners (Urhahn and Spieth, 2014). This confirmation would then encourage academic in-stitutions and industrial partners to form technological collaborations, helping companies get additional funding outside of government sub-sidies (Bianchi et al., 2019; Mai et al., 2024). Furthermore, government subsidies might benefit firms by reducing the risk and expense of their inventions and administration companies might gain from supportive regulations, which would improve performance (Liao and Yu, 2012). Therefore, it can be hypothesized that:

H5. GS positively influences business performance.

1.6. Open innovation and business performance

Companies in the Industry 4.0 sector often must adopt open inno-vation to remain competitive in volatile markets (Biscotti et al., 2018;

Singh et al., 2021). OI provides significant advantages, including improved performance metrics and enhanced technological capabilities (Hossain and Kauranen, 2016; Kraus et al., 2020; Torres de Oliveira et al., 2022). For SMEs, these practices are particularly beneficial as they facilitate entry into new markets and accelerate product launches (Carrasco-Carvajal et al., 2023; Torchia and Calabro, 2019).

Strong connections with external channels boost the effectiveness of inbound open innovation, thereby improving organizational perfor-mance (C. L. Wang et al., 2015). The dual reliance on IOI and OOI to enhance performance van de Vrande et al. (2009). While IOI involves leveraging external knowledge to develop technology (Parida et al., 2012), fostering innovative problem-solving and market opportunities (Hung and Chou, 2013), OOI helps organizations gain financial and non-financial benefits from their existing knowledge and technologies, reducing obsolescence and maintaining competitiveness (Hung and Chou, 2013).

Research indicates that firms engage in both pecuniary (e.g., pur-chasing, licensing) and non-pecuniary (e.g., external R&D cooperation) forms of IOI to meet customer needs and outcompete rivals (Singh et al., 2021) SMEs using outbound OI often seek direct monetary gains from commercializing internally developed innovations and prefer activities like venturing spinoffs and outward IP licensing (Popa et al., 2017; van de Vrande et al., 2009). Open innovation thus enhances innovation performance and productivity (Greco et al., 2021; Z. Liu et al., 2022; Lyu et al., 2020), increases the likelihood of groundbreaking ideas and business growth (Sengupta and Sena, 2020). Given these insights, it can be hypothesized that:

H6. OI positively influences business performance.

Figure 1 presents the conceptual model of this study, illustrating the relationships between social capital, dynamic capabilities, open inno-vation, and government support, along with their collective influence on business performance in Vietnamese firms. Notably, social capital, open innovation, and dynamic capabilities are represented as second-order constructs, reflecting their multi-dimensional structure.

1. Methodology

1.1. Data collection

This project received approval from the Center For Public Adminis-tration Ethics Committee (CFPA-RC-01-11-23) before the data- gathering process commenced. Furthermore, the participants' agree-ment was obtained (CFPA-RC-01-11-23). The study aimed to explore the connections between social capital, open innovation, dynamic ca-pacities, government assistance, and company performance. We collected data using a survey-based method.

To ensure the questionnaire was appropriate for the Vietnamese context, two English instructors translated the original questionnaire into Vietnamese and adjusted the items for cultural relevance. The au-thors then conducted two group discussions with seven firm directors and three government officials to gather feedback and refine the ques-tionnaire. Following this, a pilot test was conducted with 40 firm managers, which resulted in minor revisions to ensure the questions aligned with the research context.

The survey targeted business leaders, specifically firm directors and managers, as these individuals are typically responsible for strategic decision-making within their firms. Since the firm served as the unit of analysis in this study, a representative from each firm, either a senior manager or a member of the board of directors, was selected to partic-ipate. Respondents were chosen based on their ability to provide informed insights into their firm's decision-making processes.

Table A1 in the appendix provides a detailed overview of the specific modifications made to the questionnaire. To gather data, the authors, with support from industrial zone management boards in Dong Nai, Binh Duong, and Ho Chi Minh City, accessed a list of 800 potential firms. Between November 2023 and April 2024, a random sample of 450 firms was selected, yielding 289 valid responses for analysis.

1.2. Measurement

A five-point Likert scale (from1= strongly disagree to 5 = strongly agree) was used to evaluate all constructs. The questionnaire items were adapted from previous studies. The first section collected demographic data (industry type, job title, firm age, number of employees), while the second covered the constructs and their measurement items.

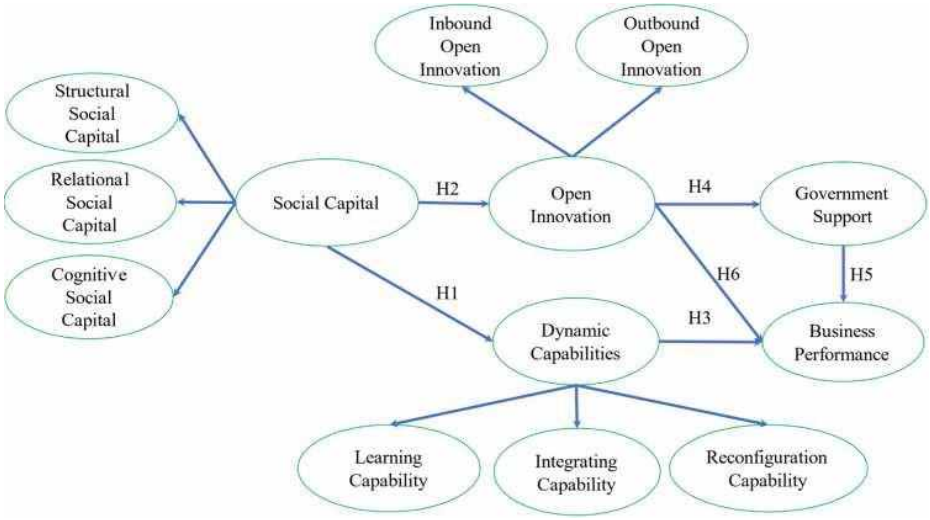

Figure 1. The research model, Source: Authors' own work.

First, social capital was built as a second-order construct, including SSC, RSC and CSC was adapted from a previous study (Allameh, 2018). Second, DC were built as a second-order construct (Farzaneh et al., 2022). Third, GS with a four-item scale was adapted from Hasan et al. (2021). Fourth, OI considered as a second-order construct included IOI and OOI, measured by an eleven-item scale adapted from prior studies (Annamalah et al., 2023; Carrasco-Carvajal et al., 2023). Business per-formance was measured by a four-item scale adapted from previous studies (Truong et al., 2024; Truong and Nguyen, 2024). Table A1 in the Appendix describes the measurement of all variables.

1.3. Method

The data was analyzed, and the research model was evaluated using Partial Least Squares-Structural Equation Modeling (PLS-SEM). PLS- SEM is a statistical method that combines principal component anal-ysis and ordinary least squares regression to evaluate partial model structures based on variance (Hair et al., 2020). PLS-SEM is useful for confirming connections in the proposed

theoretical model and investi-gating causal relationships between multiple factors. It prioritizes the acceptance or rejection of hypotheses and follows validation standards.

1. Results

1.1. Demographic characteristics

Regarding to the sample for this study comprises 289 respondents from various companies from the 42 observed variables in the model construction of this paper. When considering the number of employees, the sample includes a diverse range of company sizes. This demographic distribution provides a comprehensive view of the varied organizational characteristics within the sample, as summarized in Table 1.

1.2. Common method bias

The methodology used in this study may introduce the risk of com-mon method bias (CMB) due to the influence of questionnaire in-structions and social desirability on respondents' answers, potentially leading to shared variance among indicators (Kock, 2015). Full collin-earity variance inflation factors (FCVIFs) are effective in detecting CMB, even in models that meet standard criteria for convergent and discrim-inant validity through confirmatory factor analysis. A model

is consid-ered free from CMB if all FCVIFs from a full collinearity test are 3.3 or below (Kock, 2015)As indicated in Table 2, the FCVIFs for all latent constructs are below the 3.3 threshold, suggesting that CMB does not impact the collected data.

1.3. Validity and reliability

The initial test results, shown in Table 2, confirm the reliability and convergent validity of the constructs. Convergent and discriminant validities were evaluated using multitrait-multimethod matrix analyses (Lucas et al., 1996). Convergent validity indicates that measures of a construct should be related, while discriminant validity shows that different constructs should not be related. Confirmatory factor analysis indicated significant validity, as all item factor cross-loadings exceeded the 0.7 threshold. Reliability was assessed using Cronbach's alpha and composite reliability (CR), both of which should be above 0.70 (Hair et al., 2020). Table 2 shows Cronbach's alpha values are well above the threshold. All variables demonstrated convergent validity with Average

Table 1

Characteristics of the respondents.

Characteristics (N=289)		**Number**	**Percentage (%**
Type of industry	Services - Trading	94	33%
	Manufacturing	195	67%
Job title	Board of directors	89	31 %
	Managers	200	69 %
Firm age	5-10 years	80	28 %
	11-15 years	68	24 %
	More than 15 years	141	49 %
Number of employees	Less 100	12	4%
	101-200	15	5%
	201-300	32	11 %
	301-400	45	16%
	401-500	94	33 %
	More than 500	91	31 %

Source: Authors' own work

Variance Extracted (AVE) values above 0.5, confirming the constructs' validity.

Discriminant validity was established using the heterotrait-monotrait ratio (HTMT), with values below 0.85, meeting the criteria (Sarstedt et al., 2014). Table 3 reports these findings, verifying that all indicators are valid and satisfy both convergent and discriminant val-idity requirements.

1.4. Hypothesis testing

Table 4 presents the hypothesis testing results. A hypothesis is deemed valid if the p-value is equal to or less than 0.05 or if the accompanying t-value is more than 1.96. Otherwise, it is considered invalid and rejected. All hypotheses are supported.

1.5. Mediation effect

In examining the particular indirect effect and relying on the direct support of H1, we tested mediation to determine whether DC mediated the relationship between SC and business performance. The findings show a significant positive correlation with **B** = 0.112 and a p-value of 0.009. Moreover, the mediation effect of OI reveals that SC is signifi-cantly associated with GS (**B** = 0.209, p-value = 0.000), whereas the impact of SC on business performance through the mediation effect of OI was not found (**B** = 0.028, p-value = 0.380). Finally, GS partially me-diates the link between OI and business performance (**B** = 0.157, p-value = 0.000).

1.6. Discussions

Investigating 289 respondents from various companies in Vietnam, this study offers significant insights into the relationships between social capital, dynamic capabilities, open innovation, government support, and business performance. These factors ultimately result in more effective business outcomes. The SCT explains how social capital-—comprising relational, structural, and cognitive dimen-sions—functions within organizations. GS allows businesses to overcome their lack of funding and resources, leading to faster devel-opment and better commercial outcomes (Akintimehin et al., 2019; Annamalah et al., 2023; Nahapiet and Ghoshal, 1998; Ozanne et al., 2022).

First, SC has a significant positive direct effect on DC (supporting H1). This result underscores the importance of social capital in fostering dynamic capabilities within organizations. The strong social networks and relationships that constitute social capital likely enhance the ability of organizations to adapt, innovate, and respond to changes in the business environment. These capabilities include learning, reconfigu-ration, and integration (Fainshmidt and Frazier, 2017; Martinelli et al., 2018; Teece et al., 1997; Zhang et al., 2023). Moreover, the indirect effect of SC on business performance through dynamic capabilities is significant. This finding highlights that DC are an essential mechanism through which SC enhances business performance. Organizations with strong SC can better develop and leverage DC, thereby improving their business performance.

Second, the study confirms the positive direct effect of social capital (SC) on open innovation (OI), supporting H2. This finding is consistent with prior research (Alshahrani et al., 2024; Annamalah et al., 2023; Ju, 2023; Roh et al., 2021), which emphasizes the pivotal role of SC in fostering OI. Organizations with strong SC are better equipped to leverage external knowledge and collaborate with partners, which are essential components of open innovation. Moreover, SC positively in-fluences government support (GS) through OI, as firms engaged in OI tend to attract greater government backing. However, the indirect effect of SC on business performance through OI is not significant (as shown in Table 5). This suggests that while social capital (SC) facilitates open innovation (OI), the relationship between OI and business performance

Construct	Code	Mean	SD	Loading (> 0.7)	Alpha (> 0.7)	CR (>0.7)	AVE (>0.5)	FCVIF (<3.3)
Social Capital (second-order construct)								
Cognitive Social Capital (CSC)					0.864	0.908	0.711	2.431
	CSC1	3.913	0.778	0.808				
	CSC2	3.758	0.796	0.853				
	CSC3	3.945	0.756	0.868				
	CSC4	3.975	0.757	0.843				
Relational Social Capital (RSC)					0.907	0.935	0.782	2.274
	RSC1	4.121	0.717	0.864				
	RSC2	4.066	0.695	0.903				
	RSC3	4.097	0.699	0.900				
	RSC4	4.069	0.693	0.870				
Structural Social Capital (SSC)					0.873	0.913	0.726	2.064

SSC1	4.136	0.712	0.792				
SSC2	3.945	0.674	0.898				
SSC3	3.927	0.680	0.873				
SSC4	3.986	0.681	0.841				
Business Performance (BP)				0.884	0.915	0.682	1.103
BP1	4.083	0.762	0.802				
BP2	4.163	0.724	0.844				
BP3	4.152	0.728	0.848				
BP4	4.080	0.765	0.845				
BP5	4.055	0.783	0.788				
Government Support (GS)				0.929	0.950	0.825	1.354
GS1	3.761	0.901	0.871				
GS2	3.813	0.852	0.921				
GS3	3.841	0.837	0.932				
GS4	3.844	0.840	0.909				
Integrating Capability (IC)				0.850	0.909	0.770	1.296
IC1	3.837	0.788	0.881				
IC2	3.862	0.786	0.902				
IC3	3.938	0.782	0.849				
Learning Capability (LC)				0.839	0.892	0.675	1.373
LC1	4.031	0.722	0.775				
LC2	3.931	0.745	0.814				
LC3	3.917	0.811	0.848				
LC4	3.768	0.839	0.846				
Reconfiguration Capability (RC)				0.830	0.898	0.746	1.143
RC1	4.024	0.764	0.845				
RC2	3.903	0.714	0.899				
RC3	3.907	0.745	0.846				
Open Innovation (second-order construct)							
Inbound Open Innovation (IOI)				0.906	0.928	0.682	1.550
IOI1	3.952	0.756	0.807				
IOI2	3.882	0.832	0.850				
IOI3	3.879	0.786	0.847				
IOI4	3.893	0.784	0.861				
IOI5	3.696	0.830	0.828				
IOI6	3.765	0.828	0.758				
Outbound Open Innovation (OOI)				0.897	0.924	0.709	1.559
OOI1	3.806	0.818	0.809				
OOI2	3.806	0.838	0.868				
OOI3	3.844	0.836	0.898				
OOI4	3.875	0.806	0.827				
OOI5	3.869	0.842	0.802				

Source: Authors own work.

(H6) may be more complex than initially understood. It likely involves other mediating factors, such as cultural factors or capabilities that were not fully captured in this study beyond those already considered in the model.

Furthermore, while OI significantly influences government support (GS), its direct effect on business performance is found to be significant but relatively weaker compared to the indirect effect through GS ($B = 0.473$, $p < 0.001$). This finding indicates that the impact of OI on per-formance may manifest primarily through its ability to secure essential resources like funding and infrastructure from government initiatives, rather than directly improving performance. In emerging markets like Vietnam, where firms often face constraints such as limited absorptive capacity (Truong and Nguyen, 2024), the immediate gains from OI may be restricted.

Third, the study confirms that dynamic capabilities positively impact business performance (supporting H3). This relationship underscores the critical role of DC in driving organizational success. This finding emphasizes the importance of investing in and nurturing DC as a means of achieving sustained competitive advantage (Eikelenboom and de Jong, 2019; Protogerou et

al., 2012; Teece, 2007). Furthermore, the direct effect of OI on business performance is also significant, high-lighting the importance of innovative practices in driving organizational success. OI, which involves leveraging external knowledge and collab-orating with external partners, can lead to the development of new

Table 3 HTMT ratio and Fornell-Larcker criteria.

Variables	BP	CSC	GS	IOI	IC	LC	OOI	RC	RSC	SSC
BP										
CSC	0.345									
GS	0.455	0.316								
IOI	0.334	0.446	0.505							
IC	0.340	0.611	0.331	0.534						
LC	0.377	0.665	0.387	0.537	0.758					
OOI	0.320	0.469	0.418	0.674	0.470	0.433				
RC	0.331	0.549	0.334	0.566	0.784	0.633	0.383			
RSC	0.404	0.771	0.256	0.313	0.412	0.544	0.411	0.405		
SSC	0.371	0.719	0.264	0.343	0.399	0.541	0.421	0.373	0.832	
Fornell-Lacker criteria										
Variables	BP	CSC	GS	IOI	IC	LC	OOI	RC	RSC	SSC
BP	0.826									
CSC	0.304	0.843								
GS	0.433	0.284	0.908							
IOI	0.304	0.396	0.463	0.826						
IC	0.298	0.524	0.295	0.468	0.878					
LC	0.323	0.565	0.340	0.470	0.644	0.821				
OOI	0.288	0.412	0.381	0.617	0.413	0.379	0.842			
RC	0.286	0.462	0.293	0.490	0.661	0.532	0.332	0.864		
RSC	0.360	0.684	0.235	0.284	0.363	0.474	0.369	0.352	0.884	
SSC	0.324	0.626	0.239	0.306	0.345	0.461	0.370	0.319	0.740	0.8 5

Notes: Business performance (BP), Cognitive Social Capital (CSC), Relational Social Capital (RSC), Structural Social Capital (SSC), Government Support (GS), Inte-grating Capability (IC), Learning Capability (LC), Reconfiguration Capability (RC), Inbound Open Innovation (IOI), Outbound Open Innovation (OOI) Source: Authors' own work

Table 4

Hypothesis testing results.

	Hypothesis	Estimates (B)	T- values	P- values	Result
H1	Social Capital Dynamic capabilities	0.556	11,083	0.000	Supported
H2	Social Capital Open Innovation	0.442	7.788	0.000	Supported
H3	Dynamic capabilities Business Performance	0.197	2828	0.005	Supported
H4	Open Innovation Government Support	0.473	8.992	0.000	Supported
H5	Government Support Business Performance	0.331	4.491	0.000	Supported
H6	Open Innovation Business Performance	0.221	3.287	0.001	Supported

Source: Authors' own work

Table 5

Mediating effects.

Specific Indirect Effects	Type	B	P- values	Remark
H1. Social Capital Dynamic capabilities	Direct	0.556	0.005	Supported
Social Capital Dynamic capabilities Business Performance	Indirect	0.112	0.009	Complementary
H2. Social Capital Open Innovation	Direct	0.442	0.003	Supported

	Indirect	0.028	0.380	Unsupported
Social Capital Open Innovation Business Performance				
	Indirect	0.209	0.000	Complementary
Social Capital Open Innovation Government Support				
H4. Open Innovation Government Support	Direct	0.473	0.000	Supported
Open Innovation Government Support Business Performance	Indirect	0.157	0.000	Complementary

Source: Authors' own work products, services, and processes that enhance business performance (Carrasco-Carvajal et al., 2023; Popa et al., 2017; Singh et al., 2021; Torres de Oliveira et al., 2022).

Fourth, the study confirms that open innovation (OI) has a significant positive effect on government support, supporting H4. Firms that engage in OI by collaborating with external partners and sharing knowledge align with government policies focused on fostering innovation and economic growth. Governments often prioritize supporting these firms by providing critical resources, financial aid, and infrastructure (Cano-Kollmann et al., 2017; Chesbrough and Bogers, 2014; Jugend et al., 2018, 2020). While government support is an external factor, it is not entirely beyond a firm's control. Firms can actively position them-selves to benefit from government programs by aligning their innovation activities with public policy objectives. Therefore, although government support originates externally, firms can influence the extent of support they receive. Moreover, the indirect effect of OI on business performance through government support is significant. This finding suggests that government support is a vital intermediary through which OI contrib-utes to business performance. Firms that engage in OI are more likely to receive government support, which in turn enhances their business performance.

Finally, the study finds that government support has a significant positive effect on business performance, supporting H5. Although gov-ernment support is an external factor, firms can strategically align their internal capabilities, such as dynamic capabilities and innovation ef-forts, with the opportunities provided by this support to enhance their performance. While firms do not directly control government support, they can actively adjust their internal processes to make the most of the resources and infrastructure that government initiatives offer. In this context, government support acts not as a controllable variable but as a facilitator that amplifies the impact of a firm's internal resources on performance. This finding suggests that, while government support is external, firms can still optimize its benefits by integrating it into their strategic planning, thus indirectly enhancing their ability to leverage internal capabilities. By creating a favorable environment for innovation and business growth, government support plays a vital enabling role in driving improved business outcomes (Hasan et al., 2021; Jugend et al., 2018; Mai et al., 2024).

1. Conclusions, contributions and limitations

1.1. Conclusions

This study provides fresh insights into how the combined forces of social capital, dynamic capabilities, open innovation, and government support drive business performance. The research extends the resource-based view and dynamic capabilities theory by demonstrating that so-cial capital fosters both open innovation and dynamic capabilities, enabling firms to adapt better, innovate, and respond to changing market conditions. It also contributes to institutional theory by high-lighting the critical role of government support as a mediator, ampli-fying the benefits of open innovation, particularly in emerging markets like Vietnam. The findings confirm that dynamic capabilities exert the strongest direct influence on business performance, underscoring the importance of building internal capabilities to sustain competitive advantage. Although open

innovation also contributes directly to per-formance, its impact is most significant when firms can leverage gov-ernment support, which provides essential resources such as funding and infrastructure. Moreover, social capital is pivotal in promoting both dynamic capabilities and open innovation, creating the relational net-works necessary for innovation and adaptability. However, the indirect effect of social capital on business performance through open innovation is more complex and limited, suggesting that open innovation alone may not be sufficient to drive performance without the support of dynamic capabilities and government resources.

1.1. Theoretical contributions

This study makes several contributions to the development of social capital theory by exploring its relationship with business performance in connection with DC, OI, and GS in the context of Vietnam. The findings clarify how social capital facilitates

innovation through social connec-tions, trust, and shared norms, enhances dynamic market capabilities, and drives business success.

First, the research extends the understanding of dynamic capabilities by emphasizing their complementary role in the relationship between social capital and business performance. DC emerges as a critical mechanism through which firms leverage SC to gain a competitive advantage and improve performance in rapidly changing business environments.

Second, the study contributes to OI literature by demonstrating the direct impact of SC on OI and the critical link between OI and GS. It also uncovers the indirect pathways through which OI connects SC and GS, offering valuable insights for government bodies aiming to harness open innovation strategies to boost competitiveness and innovation capacity.

Finally, the research provides empirical evidence of the direct effect of OI on GS and its subsequent positive impact on business performance. These findings highlight the importance of supportive government policies in fostering innovation ecosystems and driving economic development. Policymakers can use these insights to design and imple-ment effective innovation policies that promote collaboration, knowl-edge exchange, and investment in innovation activities.

1.2. Practical implications

By leveraging SC, fostering DC, embracing OI, and aligning with a supportive government, businesses can enhance their innovation ca-pacity and competitiveness, driving sustained growth in Vietnam's dy-namic business environment.

First, nurturing social capital is crucial. This can be achieved by creating collaborative environments, encouraging networking, and promoting a culture of knowledge-sharing among employees. Strong SC fosters organizational resilience, facilitates the exchange of ideas, and supports cohesive teamwork, which in turn drives innovation.

Second, firms should invest in DC to respond effectively to changing market conditions and seize emerging opportunities. Building DC in-volves fostering continuous learning, encouraging agility in decision-making, and promoting experimentation. This allows firms to navigate disruptions, innovate, and maintain a competitive advantage.

Third, embracing OI enables firms to tap into external knowledge and collaborate with industry partners. Establishing strategic partner-ships, participating in innovation ecosystems, and utilizing digital platforms for collaboration are essential. OI accelerates innovation, re-duces time-to-market, and strengthens competitive positioning. More-over, engaging with government initiatives supporting innovation and economic growth is essential. Active participation in industry consul-tations, advocating favorable policies, and collaborating with govern-ment agencies and research institutions can provide businesses with access to funding, regulatory support, and infrastructure, all of which are vital for fostering innovation and business growth.

1.3. Limitation and further study

While this study offers valuable insights into the relationships among social capital (SC), dynamic capabilities (DC), open innovation (OI), and government support (GS), it has several limitations. First, the reliance on self-reported data introduces potential response bias, as participants may overestimate their firms' capabilities or performance. Second, the sample is limited to firms in manufacturing and service-trading sectors within Vietnam, which may not fully represent other industries, particularly high-tech sectors such as information technology or advanced manufacturing. These sectors may experience different inno-vation processes, regulatory pressures, and cultural dynamics that are not fully captured in this study. Additionally, cultural factors specific to Vietnam, such as a reliance on informal networks and relationship-based business practices, may limit the generalizability of the findings to other countries or regions with different cultural norms and business environments.

To improve the generalizability of the findings, future research should adopt longitudinal designs and random sampling from a wider range of industries, including high-tech sectors and firms from different cultural backgrounds. Investigating how the relationships between SC, DC, OI, GS, and business performance vary across industries and cultural contexts will offer a more comprehensive understanding of these dy-namics. Moreover, future studies should explore the role of absorptive capacity, external regulatory factors, and cultural influences as media-tors or moderators of these relationships. This broader approach would deepen theoretical insights and enhance the practical implications for businesses and policymakers, particularly in emerging markets.

Funding

This research does not receive any financial support.

CRediT authorship contribution statement

Dien Van Tran: Writing - review & editing, Writing - original draft, Project administration, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization. **Thang Nam Huynh:** Writing - original draft, Resources, Project administration, Methodol-ogy, Data curation. **Khanh Van Ma:** Writing - review & editing, Project administration, Investigation, Data curation. **Phuong Van Nguyen:** Writing - review & editing, Writing - original draft, Supervision, Re-sources, Project administration, Methodology, Data curation, Concep-tualization. **Nhi Tran Thao Dinh:** Writing - review & editing, Writing - original draft, Visualization, Validation, Software, Data curation.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence

Table A1 Measurement items

Construction (Source)	Code	Measurement	Modification
Social capital (SC) (Allameh, 2018) **Structural social capital**	**SSC1**	In my organization, I have a very good relationship with my colleagues.	No change
	SSC2	My colleagues know what knowledge I have at my disposal.	Major modification
	SSC3	I know what knowledge could be relevant to which colleague.	Major modification
	SSC4	Within my organization, I know who has knowledge that is relevant to me at their disposal.	Major modification
Relational social capital	**RSC1**	I feel connected to my colleagues.	
	RSC2	I know my colleagues will always try and help me out if I get into difficulties.	No change
	RSC3	I can trust my colleagues to lend me a hand if I need it.	Major modification
	RSC4	I can rely on my colleagues when I need support in my work.	No change
Cognitive social capital	**CSC1**	My colleagues and I always agree on what is important at work.	Major modification
	CSC2	My colleagues and I always share the same ambitions and vision at work.	No change
	CSC3	My colleagues and I are always enthusiastic about pursing the collective goals and missions of the whole organization.	No change
	CSC4	The culture and management style of our organization is very similar to ours.	No change
Dynamic capabilities			
Learning capability	**LC1**	We are constantly learning within the organization.	No change
	LC2	In our company, the process of knowledge creation and development takes place according to the requirements of the units.	Major modification
	LC3	We are constantly setting up training teams.	Major modification
	LC4	We have ongoing cross-department training programs.	Major modification
Integrating capability	**IC1**	Our company focuses on gathering customer information and discovering potential markets.	No change
	IC2	Our company utilizes the specialized services of other organizations in its management decisions.	Major modification
	IC3	Our company focuses on technologies related to the our industry to develop new products.	Major modification
Reconfiguration capability	**RC1**	Our company focuses on reorganizing jobs and creating new job opportunities.	Major modification
	RC2	Our company reacts quickly to market changes.	No change
	RC3	Our company responds to its competitors in a timely manner.	No change
	RC4	We have effective and efficient communication with partner organizations.	No change

Construction (Source)	Code	Measurement	Modification

Government Support(Hasan et al., 202)	**GS1**	Digital transformation receives financial support from the government or relevant agencies. change	No	
	GS2	The government issues relevant policies to promote digital transformation in enterprises. change	No	
	GS3	Firms recognize that there is legal support for the application of digital transformation. change	No	
	GS4	Existing laws and regulations are sufficient to protect enterprises in applying the digital transformation. change		No
	GS5	Digital transformation receives financial support from the government or relevant agencies. change	No	

References

Achidi Ndofor, H., Priem, R.L., 2011. Immigrant entrepreneurs, the ethnic enclave strategy, and venture performance. J. Manag. 37 (3), 790-818. https://doi.org/ 10.1177/0149206309345020.

Agyapong, F.O., Agyapong, A., Poku, K., 2017. Nexus between social capital and performance of micro and small firms in an emerging economy: the mediating role of innovation. Cogent Bus. Manag. 4 (1), 1309784. https://doi.org/10.1080/ 23311975.2017.1309784.

Akintimehin, O.O., Eniola, A.A., Alabi, O.J., Eluyela, D.F., Okere, W., Ozordi, E., 2019. Social capital and its effect on business performance in the Nigeria informal sector. Heliyon 5 (7). https://doi.org/10.1016/j.heliyon.2019.e02024.

Allameh, S.M., 2018. Antecedents and consequences of intellectual capital. J. Intellect. Cap. 19 (5), 858-874. https://doi.org/10.1108/JIC-05-2017-0068.

Al-Omoush, K.S., Ribeiro-Navarrete, S., Lassala, C., Skare, M., 2022. Networking and knowledge creation: Social capital and collaborative innovation in responding to the COVID-19 crisis. J. Innov. Knowl. 7 (2), 100181. https://doi.org/10.1016/j. jik.2022.100181.

Alshahrani, I., Al-Jayyousi, O., Aldhmour, F., Alderaan, T., 2024. Towards understanding the influence of innovative work behavior on healthcare organizations' performance: the mediating role of transformational leaders. Arab Gulf J. Sci. Res. 42 (1), 198-216. https://doi.org/10.1108/AGJSR-09-2022-0167.

Al-Tit, A.A., Al-Ayed, S., Alhammadi, A., Hunitie, M., Alsarayreh, A., Albassam, W., 2022. The impact of employee development practices on human capital and social capital: the mediating contribution of knowledge management. J. Open Innov.: Technol., Mark., Complex. 8 (4), 218. https://doi.org/10.3390/JOITMC8040218.

Alyahya, M.A., Mohamed, E., Akamavi, R., Elshaer, I.A., Azzaz, A.M.S., 2020. Can cognitive capital sustain customer satisfaction? The mediating effects of employee self-efficacy. J. Open Innov.: Technol. Mark. Complex. 6 (4), 191. https://doi.org/ 10.3390/JOITMC6040191.

Annamalah, S., Paraman, P., Ahmed, S., Dass, R., Sentosa, I., Pertheban, T.R., Shamsudin, F., Kadir, B., Aravindan, K.L., Raman, M., Hoo, W.C., Singh, P., 2023. The role of open innovation and a normalizing mechanism of social capital in the tourism industry. J. Open Innov.: Technol. Mark. Complex. 9 (2), 100056. https:// doi.org/10.1016/j.joitmc.2023.100056.

Augusto Felicio, J., Couto, E., Caiado, J., 2014. Human capital, social capital and organizational performance. Manag. Decis. 52 (2), 350-364. https://doi.org/ 10.1108/MD-04-2013-0260.

Bianchi, M., Murtinu, S., Scalera, V.G., 2019. R&D subsidies as dual signals in technological collaborations. Res. Policy 48 (9), 103821. https://doi.org/10.1016/j. respol.2019.103821.

Biscotti, A.M., Mafrolla, E., Giudice, M., Del, D'Amico, E., 2018. CEO turnover and the new leader propensity to open innovation: agency-resource dependence view and social identity perspective. Manag. Decis. 56 (6), 1348-1364. https://doi.org/ 10.1108/MD-04-2017-0392/FULL/XML.

Bogers, M., Chesbrough, H., Moedas, C., 2018. Open innovation: research, practices, and policies. Calif. Manag. Rev. 60 (2), 5-16. https://doi.org/10.1177/ 0008125617745086.

Bolino, M.C., Turnley, W.H., Bloodgood, J.M., 2002. Citizenship behavior and the creation of social capital in organizations. Acad. Manag. Rev. 27 (4), 505-522. https://doi.org/10.5465/amr.2002.7566023.

Cano-Kollmann, M., Hamilton, R.D., Mudambi, R., 2017. Public support for innovation and the openness of firms' innovation activities. Ind. Corp. Change 26 (3), 421-442. https://doi.org/10.1093/ICC/DTW025.

Carrasco-Carvajal, O., García-Perez-de-Lema, D., Castillo-Vergara, M., 2023. Impact of innovation strategy, absorptive capacity, and open innovation on SME performance: a Chilean case study. J. Open Innov.: Technol., Mark. Complex. 9 (2), 100065. https://doi.org/10.1016/j.joitmc.2023.100065.

Carson, E., Ranzijn, R., Winefield, A., Marsden, H., 2004. Intellectual capital: mapping employee and work group attributes. J. Intellect. Cap. 5 (3), 443-463. https://doi. org/10.1108/14691930410550390.

Cheah, S.L.-Y., Ho, Y.-P., 2020. Effective industrial policy implementation for open innovation: the role of government resources and capabilities. Technol. Forecast. Soc. Change 151 (3)), 119845. https://doi.org/10.1016/j.techfore.2019.119845.

Cheng, C.C.J., Chen, J.S., 2013. Breakthrough innovation: the roles of dynamic innovation capabilities and open innovation activities. J. Bus. Ind. Mark. 28 (5), 444-454. https://doi.org/10.1108/08858621311330281/FULL/XML.

Chesbrough, H., Bogers, M., 2014. Explicating open innovation. New Frontiers in Open Innovation. Oxford University Press. https://doi.org/10.1093/acprofoso/ 9780199682461.003.0001.

Choi, J.J., Jiang, C., Shenkar, O., 2015. The quality of local government and firm performance: the case of China's Provinces. Manag. Organ. Rev. 11 (4), 679-710. https://doi.org/10.1017/mor.2015.46.

Chow, W.S., Chan, L.S., 2008. Social network, social trust and shared goals in organizational knowledge sharing. Inf. Manag. 45 (7), 458-465. https://doi.org/ 10.1016/j.im.2008.06.007.

Cricelli, L., Grimaldi, M., Vermicelli, S., 2022. Crowdsourcing and open innovation: a systematic literature review, an integrated framework and a research agenda. Rev. Manag. Sci. 16 (5), 1269-1310. https://doi.org/10.1007/s11846-021-00482-9.

Dai, W. (David), Mao, Z. (Eddie), Zhao, X. (Roy), Mattila, A.S., 2015. How does social capital influence the hospitality firm's financial performance? The moderating role of entrepreneurial activities. Int. J. Hosp. Manag. 51, 42-55. https://doi.org/ 10.1016/j.ijhm.2015.08.011.

van de Vrande, V., de Jong, J.P.J., Vanhaverbeke, W., de Rochemont, M., 2009. Open innovation in SMEs: trends, motives and management challenges. Technovation 29 (6-7), 423-437. https://doi.org/10.1016/J.TECHNOVATION.2008.10.001.

Doh, S., Kim, B., 2014. Government support for SME innovations in the regional industries: the case of government financial support program in South Korea. Res. Policy 43 (9), 1557-1569. https://doi.org/10.1016/J.RESPOL.2014.05.001.

Eikelenboom, M., de Jong, G., 2019. The impact of dynamic capabilities on the sustainability performance of SMEs. J. Clean. Prod. 235, 1360-1370. https://doi. org/10.1016/j.jclepro.2019.07.013.

Eisenhardt, K.M., Martin, J.A., 2000. Dynamic capabilities: what are they? Strateg. Manag. J. 21 (10-11), *1105-1121*.

Fainshmidt, S., Frazier, M.L., 2017. What facilitates dynamic capabilities? The role of organizational climate for trust. Long. Range Plan. 50 (5), 550-566. https://doi.org/ 10.1016/j.lrp.2016.05.005.

Farzaneh, M., Wilden, R., Afshari, L., Mehralian, G., 2022. Dynamic capabilities and innovation ambidexterity: the roles of intellectual capital and innovation orientation. J. Bus. Res. 148, 47-59. https://doi.org/10.1016/j.jbusres.2022.04.030.

Fernandez-Pinto, H., Duarte, C.A.M., Villamizar, S.P., Suarez, J.E.S., 2024. Horizontal innovation: the core of open innovation in the construction of the dynamic capacities in the Colombian industry. J. Open Innov.: Technol. Mark. Complex. 10 (1), 100229. https://doi.org/10.1016/J.JOITMC.2024.100229.

Ferraris, A., Santoro, G., Bresciani, S., 2017. Open innovation in multinational companies' subsidiaries: the role of internal and external knowledge. Eur. J. Int. Manag. 11 (4), 452. https://doi.org/10.1504/EJIM.2017.085583.

Gassmann, O., Enkel, E., Chesbrough, H., 2010. The future of open innovation. RD

Manag. 40 (3), 213-221. https://doi.org/10.1111/J.1467-9310.2010.00605.X.

Gogan, L.M., Duran, D.C., Draghici, A., 2015. Structural capital - a proposed measurement model. Procedia Econ. Financ. 23, 1139-1146. https://doi.org/ 10.1016/S2212-5671(15)00503-1.

Greco, M., Grimaldi, M., Cricelli, L., 2016. An analysis of the open innovation effect on firm performance. Eur. Manag. J. 34 (5), 501-516. https://doi.org/10.1016/J. EMJ.2016.02.008.

Greco, M., Grimaldi, M., Locatelli, G., Serafini, M., 2021. How does open innovation enhance productivity? An exploration in the construction ecosystem. Technol. Forecast. Soc. Change 168, 120740. https://doi.org/10.1016/J.TECHFORE.2021.120740.

Gupta, A.K., Gupta, N., 2019. Innovation and culture as a dynamic capability for firm performance: a study from emerging markets. Glob. J. Flex. Syst. Manag. 20 (4), 323-336. https://doi.org/10.1007/s40171-019-00218-5.

Hair, J.F., Howard, M.C., Nitzl, C., 2020. Assessing measurement model quality in PLS- SEM using confirmatory composite analysis. J. Bus. Res. 109, 101-110. https://doi. org/10.1016/j.jbusres.2019.11.069.

Hasan, S., Ali, M., Kurnia, S., Thurasamy, R., 2021. Evaluating the cyber security readiness of organizations and its influence on performance. J. Inf. Secur. Appl. 58, 102726. https://doi.org/10.1016/j.jisa.2020.102726.

Holl, A., Rama, R., 2012. Technology sourcing: Are biotechnology firms different? An exploratory study of the Spanish case. Sci. Public Policy 39 (3), 304-317. https:// doi.org/10.1093/scipol/scs007.

Hossain, M., Kauranen, I., 2016. Open innovation in SMEs: a systematic literature review. J. Strategy Manag. 9 (1), 58-73. https://doi.org/10.1108/JSMA-08-2014- 0072.

Huizingh, E.K.R.E., 2011. Open innovation: state of the art and future perspectives. Technovation 31 (1), 2-9. https://doi.org/10.1016/J.

TECHNOVATION.2010.10.002.

Hung, K.P., Chou, C., 2013. The impact of open innovation on firm performance: the moderating effects of internal R&D and environmental turbulence. Technovation 33 (10-11), 368-380. https://doi.org/10.1016/J.TECHNOVATION.2013.06.006.

Ju, J., 2023. How open innovation drives intellectual capital to superior organizational resilience: evidence from China's ICT sector. J. Intellect. Cap. 24 (6), 1464-1484. https://doi.org/10.1108/JIC-12-2022-0251.

Jugend, D., Jabbour, C.J.C., Alves Scaliza, J.A., Rocha, R.S., Junior, J.A.G., Latan, H., Salgado, M.H., 2018. Relationships among open innovation, innovative performance, government support and firm size: comparing Brazilian firms embracing different levels of radicalism in innovation. Technovation 74-75, 54-65. https://doi.org/10.1016/j.technovation.2018.02.004.

Jugend, D., Fiorini, P.D.C., Armellini, F., Ferrari, A.G., 2020. Public support for innovation: a systematic review of the literature and implications for open innovation. Technol. Forecast. Soc. Change 156, 119985. https://doi.org/10.1016/j.techfore.2020.119985.

Kock, N., 2015. Common method bias in PLS-SEM: a full collinearity assessment approach. Int. J. E-Collab. 11 (4), 1-10. https://doi.org/10.4018/ijec.2015100101.

Kraus, S., Breier, M., Dasí-Rodríguez, S., 2020. The art of crafting a systematic literature review in entrepreneurship research. Int. Entrep. Manag. J. 16 (3), 1023-1042. https://doi.org/10.1007/s11365-020-00635-4.

Lakse Mudiyanselage, C.S.M., 2020. Effect of social capital on firm performance: an empirical study of small enterprises in Sri Lanka. J. Soc. Sci. Res. 16, 108-125. https://doi.org/10.24297/jssr.v16i.8904.

Laursen, K., Salter, A., 2006. Open for innovation: the role of openness in explaining innovation performance among U.K. manufacturing firms. Strateg. Manag. J. 27 (2), 131-150. https://doi.org/10.1002/smj.507.

Liao, T.J., Yu, C.M.J., 2012. Knowledge transfer, regulatory support, legitimacy, and financial performance: the case of foreign firms investing in China. J. World Bus. 47 (1), 114-122. https://doi.org/10.1016/jjwb.2010.10.026.

Lichtenthaler, U., 2009. Outbound open innovation and its effect on firm performance: examining environmental influences. RD Manag. 39 (4), 317-330. https://doi.org/ 10.1111/J.1467-9310.2009.00561.X.

Liu, C.-H., 2017. The relationships among intellectual capital, social capital, and performance - the moderating role of business ties and environmental uncertainty. Tour. Manag. 61, 553-561. https://doi.org/10.1016/j.tourman.2017.03.017.

Liu, Y., Ndubisi, N.O., Liu, Y., Barrane, F.Z., 2020. New product development and sustainable performance of Chinese SMMEs: the role of dynamic capability and intra-national environmental forces. Int. J. Prod. Econ. 230, 107817. https://doi.org/ 10.1016/j.ijpe.2020.107817.

Liu, Z., Shi, Y., Yang, B., 2022. Open innovation in times of crisis: an overview of the healthcare sector in response to the COVID-19 pandemic. J. Open Innov.: Technol. Mark. Complex. 8 (1), 21. https://doi.org/10.3390/JOITMC8010021.

Lucas, R.E., Diener, E., Suh, E., 1996. Discriminant validity of well-being measures.

J. Personal. Soc. Psychol. 71 (3), 616-628. https://doi.org/10.1037/0022- 3514.71.3.616.

Luo, Y., 2000. Dynamic capabilities in international expansion. J. World Bus. 35 (4), 355-378. https://doi.org/10.1016/S1090-9516(00)00043-2.

Lyu, Y., Zhu, Y., Han, S., He, B., Bao, L., 2020. Open innovation and innovation "Radicalness"—the moderating effect of network embeddedness. Technol. Soc. 62, 101292. https://doi.org/10.1016/J.TECHSOC.2020.101292.

Mai, B.T., Nguyen, P.V., Ton, U.N.H., Ahmed, Z.U., 2024. Government policy, IT capabilities, digital transformation, and innovativeness in Post-Covid context: case of Vietnamese SMEs. Int. J. Organ. Anal. 32 (2), 333-356. https://doi.org/10.1108/ IJOA-11-2022-3480.

Marcus, A.A., Anderson, M.H., 2006. A general dynamic capability: does it propagate business and social competencies in the retail food industry? J. Manag. Stud. 43 (1), 19-46. https://doi.org/10.1111/j.1467-6486.2006.00581.x.

Martinelli, E., Tagliazucchi, G., Marchi, G., 2018. The resilient retail entrepreneur: dynamic capabilities for facing natural disasters. Int. J. Entrep. Behav. Res. 24 (7), 1222-1243. https://doi.org/10.1108/IJEBR-11-2016-0386.

Mitchelmore, S., Rowley, J., 2010. Entrepreneurial competencies: a literature review and development agenda. Int. J. Entrep. Behav. Res. 16 (2), 92-111. https://doi.org/ 10.1108/13552551011026995.

Mohaghegh, M., Blasi, S., Großler, A., 2021. Dynamic capabilities linking lean practices and sustainable business performance. J. Clean. Prod. 322, 129073. https://doi.org/ 10.1016/j.jclepro.2021.129073.

Nahapiet, J., Ghoshal, S., 1998. Social capital, intellectual capital, and the organizational advantage. Acad. Manag. Rev. 23 (2), 242-266. https://doi.org/10.5465/ amr.1998.533225.

OECD. (2021). COVID-19 emergency government support and ensuring a level playing field on the road to recovery.

OECD. (2023). Government Support in Industrial Sectors: A Synthesis Report.

Otoo, C.O.A., Li, W., Pomegbe, W.W.K., Dogbe, C.S.K., 2024. Effect of internal knowledge sourcing on multinational enterprise subsidiaries' service innovation performance: the mediating role of organisational learning. Eur. J. Int. Manag. 23 (1), 60-87. https://doi.org/10.1504/EJIM.2024.138405.

Ozanne, L.K., Chowdhury, M., Prayag, G., Mollenkopf, D.A., 2022. SMEs navigating COVID-19: the influence of social capital and dynamic capabilities on organizational resilience. Ind. Mark. Manag. 104, 116-135. https://doi.org/10.1016/j.indmarman.2022.04.009.

Parida, V., Westerberg, M., Frishammar, J., 2012. Inbound open innovation activities in high-tech SMEs: the impact on innovation performance. J. Small Bus. Manag. 50 (2), 283-309. https://doi.org/10.1111/J.1540-627X.2012.00354.X.

Park, J.Y., Muaid, R., Lew, Y.K., Oh, C.H., 2023. Exploring the role of organisational learning and leadership in developing dynamic capabilities. Eur. J. Int. Manag. 19 (1), 27. https://doi.org/10.1504/EJIM.2023.127231.

Pasamar, S., Cabrales, A.L., Cabrales, R.V., 2015. Ambidexterity and intellectual capital architectures for developing dynamic capabilities: towards a research agenda. Eur. J. Int. Manag. 9 (1), 74. https://doi.org/10.1504/EJIM.2015.066672.

Patel, P.C., Terjesen, S., 2011. Complementary effects of network range and tie strength in enhancing transnational venture performance. Strateg. Entrep. J. 5 (1), 58-80. https://doi.org/10.1002/sej.107.

Pena, I., 2002. Intellectual capital and business start-up success. J. Intellect. Cap. 3 (2), 180-198. https://doi.org/10.1108/14691930210424761.

Popa, S., Soto-Acosta, P., Martinez-Conesa, I., 2017. Antecedents, moderators, and outcomes of innovation climate and open innovation: an empirical study in SMEs. Technol. Forecast. Soc. Change 118, 134-142. https://doi.org/10.1016/J.TECHFORE.2017.02.014.

Priyono, A., Hidayat, A., 2024. Fostering innovation through learning from digital business ecosystem: a dynamic capability perspective. J. Open Innov.: Technol. Mark. Complex. 10 (1), 100196. https://doi.org/10.1016/J.JOITMC.2023.100196.

Protogerou, A., Caloghirou, Y., Lioukas, S., 2012. Dynamic capabilities and their indirect impact on firm performance. Ind. Corp. Change 21 (3), 615-647. https://doi.org/ 10.1093/icc/dtr049.

Pruthi, S., Wright, M., 2017. Social ties, social capital, and recruiting managers in transnational ventures. J. East-West Bus. 23 (2), 105-139. https://doi.org/10.1080/ 10669868.2016.1270247.

Pylypenko, H.M., Pylypenko, Y.I., Dubiei, Y.V., Solianyk, L.G., Pazynich, Y.M., Buketov, V., Smolinski, A., Magdziarczyk, M., 2023. Social capital as a factor of innovative development. J. Open Innov.: Technol., Mark., Complex. 9 (3), 100118. https://doi.org/10.1016/J.JOITMC.2023.100118.

Razumovskaia, E., Yuzvovich, L., Kniazeva, E., Klimenko, M., Shelyakin, V., 2020. The effectiveness of Russian government policy to support SMEs in the COVID-19 pandemic. J. Open Innov.: Technol., Mark., Complex. 6 (4), 160. https://doi.org/ 10.3390/JOITMC6040160.

Ring, P.J., 2005. Security in pension provision: a critical analysis of UK Government Policy. J. Soc. Policy 34 (3), 343-363. https://doi.org/10.1017/ S0047279405008810.

Roh, T., Lee, K., Yang, J.Y., 2021. How do intellectual property rights and government support drive a firm's green innovation? The mediating role of open innovation.

J. Clean. Prod. 317, 128422. https://doi.org/10.1016/j.jclepro.2021.128422.

Sánchez-García, E., Marco-Lajara, B., Martínez-Falcó, J., Poveda-Pareja, E., 2023. Cognitive social capital for knowledge absorption in specialized environments: the path to innovation. Heliyon 9 (3), e14223. https://doi.org/10.1016/j.heliyon.2023. e14223.

Sarstedt, M., Ringle, C.M., Henseler, J., Hair, J.F., 2014. On the emancipation of PLS- SEM: a commentary on rigdon (2012). Long. Range Plan. 47 (3), 154-160. https:// doi.org/10.1016/j.lrp.2014.02.007.

Sengupta, A., Sena, V., 2020. Impact of open innovation on industries and firms - a dynamic complex systems view. Technol. Forecast. Soc. Change 159, 120199. https://doi.org/10.1016/j.techfore.2020.120199.

Singh, S.K., Gupta, S., Busso, D., Kamboj, S., 2021. Top management knowledge value, knowledge sharing practices, open innovation and organizational performance. J. Bus. Res. 128, 788-798. https://doi.org/10.1016/jjbusres.2019.04.040.

Srisathan, W.A., Ketkaew, C., Phonthanukitithaworn, C., Naruetharadhol, P., 2023. Driving policy support for open eco-innovation enterprises in Thailand: a probit regression model. J. Open Innov.: Technol., Mark., Complex. 9 (3), 100084. https:// doi.org/10.1016/J.JOITMC.2023.100084.

Tan, A., 2017. The effect of social capital and absorptive capacity through knowledge management on finance company performance in Indonesia. Int. Bus. Res. 11 (1), 87. https://doi.org/10.5539/ibr.v11n1p87.

Teece, D., Peteraf, M.A., Leih, S., 2016. Dynamic capabilities and organizational agility: risk, uncertainty and entrepreneurial management in the innovation economy. SSRN Electron. J. https://doi.org/10.2139/ssrn.2771245.

Teece, D.J., 2007. Explicating dynamic capabilities: the nature and microfoundations of (sustainable) enterprise performance. Strateg. Manag. J. 28 (13), 1319-1350. https://doi.org/10.1002/smj.640.

Teece, D.J., Pisano, G., Shuen, A., 1997. Dynamic capabilities and strategic management. Strateg. Manag. J. 18 (7), 509-533. https://doi.org/10.1002/(SICI)1097-0266 (199708)18:7<509::AID-SMJ882>3.0.CO;2-Z.

Torchia, M., Calabro, A., 2019. Open innovation in SMEs: a systematic literature review. J. Enterprising Cult. 27 (02), 201-228. https://doi.org/10.1142/ S0218495819500080.

Torres de Oliveira, R., Verreynne, M.-L., Figueira, S., Indulska, M., Steen, J., 2022. How do institutional innovation systems affect open innovation? J. Small Bus. Manag. 60 (6), 1404-1448. https://doi.org/10.1080/00472778.2020.1775466.

Truong, B.T.T., Nguyen, P.V., 2024. Driving business performance through intellectual capital, absorptive capacity, and innovation: the mediating influence of environmental compliance and innovation. Asia Pac. Manag. Rev. 29 (1), 64-75. https://doi.org/10.1016/j.apmrv.2023.06.004.

Truong, B.T.T., Nguyen, P.V., Vrontis, D., Inuwa, I., 2024. Exploring the interplay of intellectual capital, environmental compliance, innovation and social media usage in enhancing business performance in Vietnamese manufacturers. J. Intellect. Cap. https://doi.org/10.1108/JIC-10-2023-0233.

Tsai, W., Ghoshal, S., 1998. Social capital and value creation: the role of intrafirm networks. Acad. Manag. J. 41 (4), 464-476. https://doi.org/10.5465/257085.

Urhahn, C., Spieth, P., 2014. Governing the portfolio management process for product innovation—a quantitative analysis on the relationship between portfolio management governance, portfolio innovativeness, and firm performance. IEEE Trans. Eng. Manag. 61 (3), 522-533. https://doi.org/10.1109/TEM.2014.2327254.

Wang, C.L., Senaratne, C., Rafiq, M., 2015. Success traps, dynamic capabilities and firm performance. Br. J. Manag. 26 (1), 26-44. https://doi.org/10.1111/1467- 8551.12066.

Wang, J., 2018. Innovation and government intervention: a comparison of Singapore and Hong Kong. Res. Policy 47 (2), 399-412. https://doi.org/10.1016/j. respol.2017.12.008.

Yun, J.J., Zhao, X., Del Gaudio, G., Della Corte, V., & Sadoi, Y. (2023). Leveraging business model innovation through the dynamics of open innovation: a multi-country investigation in the restaurant industry. European Journal of Innovation Management. Online First, https://doi.org/10.1108/EJIM-07-2023-0607.

Yun, J.J., Zhao, X., Jeong, E., Ahn, H., Park, K., 2024. Micro open innovation dynamics under inter-rationality. Technol. Forecast. Soc. Change 201, 123263. https://doi. org/10.1016/j.techfore.2024.123263.

Yun, J.J., Kim, B. hwan, Zhao, X., Jeong, E., Ahn, J. gi, 2024. Open innovation signals: exploring the financial data with patents. Sci. Technol. Soc. 29 (2), 199-223. https:// doi.org/10.1177/09717218241238202.

Zhang, Y., Long, J., Zhao, W., 2023. Building dynamic capabilities of small and medium-sized enterprises through relational embeddedness: evidence from China. Electron. Commer. Res. 23 (4), 2859-2906. https://doi.org/10.1007/s10660-022-09579-z.

Zollo, M., Winter, S.G., 2002. Deliberate learning and the evolution of dynamic capabilities. Organ. Sci. 13 (3), 339-351. https://doi.org/10.1287/ orsc.13.3.339.2780.