Journal of Open Innovation: Technology, Market, and Complexity 11 (2025) 100463

Contents lists available at ScienceDirect

Journal of Open Innovation: Technology, Market, and Complexity

journal homepage: www.sciencedirect.com/journal/journal-of-open-innovation-technology-market-and-complexity

Evaluating the role of protection motivation theory in information security policy compliance: Insights from the banking sector using PLS-SEM approach

Ebrahim Mohammed Alrawhani [a], Awanis Romli [a,*], Mohammed A. Al-Sharafi [b,*]

[a] Faculty of Computing, University Malaysia Pahang Al-Sultan Abdullah, Pekan, Pahang 26600, Malaysia
[b] IRC for Finance and Digital Economy, KFUPM Business School, King Fahd University of Petroleum & Minerals, Dhahran, Saudi Arabia

ARTICLE INFO

Keywords:
Information security policy
Research model
Protection motivation theory
Compliance behaviour
Banking sector

ABSTRACT

This research investigated the behavior related to compliance with information security policy in the Yemeni banking sector by using the protection motivation theory (PMT). While PMT has been a prominent framework in understanding information security compliance, previous research has produced inconsistent findings regarding its factors' effects on compliance behavior, necessitating further empirical validation. Moreover, the majority of research has been carried out in developed countries. The data were collected from 210 bank employees in Yemen and analyzed using PLS-SEM. This research study showed that perceived self-efficacy, response efficacy, and severity significantly influence the employees' intentional behavior in complying with information security policies. However, the results did not support the hypotheses of perceived response cost and perceived vulnerability. The study also discusses both theoretical and practical implications of enhancing information security compliance behavior.

1. Introduction

Information systems (IS) are becoming more important to the continued operation of modern organizations since these systems often hold significant data and assets related to the organization (Qatawneh, 2024). Organizations commonly implement various security measures to secure these essential information system assets from unauthorized use, misuse, or damage. Some of these measures include the use of antivirus software, encryption, system backups, and comprehensive monitoring systems (Alkhudhayr et al., 2019; Koolen et al., 2024; Makeri, 2020; Shulha et al., 2022). However, these security measures only address technological or technical issues, and they are not always sufficient to keep an organization's IS resources safe (Akello, 2024; Gaurav and Panigrahi, 2022). Another security concern arises from employee noncompliance, a common issue faced by organizations that may lead to security breaches and data breaches (Gwebu et al., 2020). The rapid proliferation of emerging technologies has introduced new complexities to the cybersecurity landscape (Al-Emran et al., 2024). These technologies, while offering transformative potential across various sectors, also bring novel challenges related to privacy concerns, perceived threats, and response costs. Behavioral and cognitive factors have been shown to significantly influence cybersecurity compliance and safe practices, emphasizing that technical measures alone are insufficient to address these evolving risks (Al-Emran et al., 2025; Al-Momani et al., 2024).

The banking sector, a key industry for IS implementation, is particularly susceptible to security threats given its reliance on sensitive financial data and complex operational systems (Matkovskaya et al., 2022). The successful adoption of security measures in banking institutions hinges on technological readiness, organizational support, and environmental influences (Bany Mohammad et al., 2022). Furthermore, the dynamic nature of banking ecosystems requires institutions to adapt to emerging technologies and innovative business models to maintain competitiveness (Al-Sharafi et al., 2018; Matkovskaya et al., 2022). These advancements necessitate robust compliance with information security policies to mitigate risks while fostering innovation and operational efficiency. In Yemen, information security measures in the banks are crucial due to the sensitive customer data and financial assets managed by banks. Despite challenges like ongoing conflict and economic instability, which have heightened vulnerability to cyber-attacks (Al-Khulaidi et al., 2023), the sector has made significant progress. This improvement is driven by increased awareness among bank staff and

* Corresponding authors.
E-mail addresses: awanis@umpsa.edu.my (A. Romli), mohamed.a.alsharafi@gmail.com (M.A. Al-Sharafi).

https://doi.org/10.1016/j.joitmc.2024.100463

Available online 28 December 2024

management, investments in new security technologies, and the adoption of international security standards (Central Bank of Yemen, 2022). However, a study by (Abdualmajed et al., 2022) found that while some banks have reached an ideal maturity level in security practices, most still adhere only to fundamental security criteria, indicating a gap in comprehensive implementation. Key challenges include a shortage of skilled security personnel, limited investment resources, and a lack of a comprehensive national security strategy (Nasser et al., 2020). Nonetheless, the sector's commitment to enhancing information security is vital for protecting assets and maintaining public trust.

A critical issue in the human aspects of information security threat prevention is internal threats from employees' unintentional and intentional disclosure of sensitive information (Alghamdi, 2021). The literature suggests that individuals are often the weakest link in cybersecurity, contributing to a significant number of security breaches in businesses (Al-Momani et al., 2024; Kuzior et al., 2022; Torten et al., 2018; Yuryna Connolly et al., 2017). For this reason, scholars have increasingly focused on understanding what motivates human intent toward complying with information security policies (ISP) (Amankwa et al., 2022). One significant issue is that certain employees may decide against adhering to information security regulations and standards to expedite their tasks (Alzamil, 2018). Therefore, understanding employees' intentions to comply with ISP is vital, as it is a significant indicator of actual compliance behavior (Sas et al., 2021). Prior studies in the information security domain have shown that behavioral intentions often lead to actual compliance with ISP (AlGhamdi et al., 2022; Nasir et al., 2019). Employee's compliance intention with information security policy refers to their commitment to adhering to organizational guidelines designed to ensure the safety of information and technology resources (Hu et al., 2021).

Protection Motivation Theory (PMT) is a key framework in the literature on information security policy compliance, explaining how protective behaviors are initiated and sustained. PMT outlines two processes: "threat assessment" and "coping assessment" (Ogbanufe et al., 2023). Threat assessment evaluates the severity and likelihood of threats while coping assessment assesses one's ability to respond effectively and the associated costs (Chang et al., 2022). These processes generate "protective motivation," driving the intent to undertake protective actions (Boss et al., 2015). Thus, protective motivation links perceived threats and behavioral intentions (Ogbanufe et al., 2023). However, the existing research studies have yielded fluctuating results about the influence of PMT factors on security compliance behavior, highlighting the need for further empirical validation (Ogbanufe et al., 2023). Additionally, there is limited literature regarding PMT and information security compliance in developing nations like Yemen. This research aims to address the gap by empirically investigating the factors that influence employees' compliance with ISP in the Yemeni banking sector, using PMT as a theoretical framework. The findings contribute new insights into the application of PMT within Yemen's banking environment and offer practical implications for improving information security compliance in organizations facing similar challenges. This study specifically develops a model tailored to the Yemeni banking sector, aiming to uncover the motivations behind employees' adherence to data security regulations.

2. Employee compliance with ISP in banking sector

Employee compliance with Information Security Policies ISP is crucial for maintaining the integrity, confidentiality, and availability of sensitive financial data in the public and private sectors (Khando et al., 2021). Banking sectors face unique challenges due to the highly regulated nature of the industry and the significant consequences of data breaches, which can include financial loss, reputational damage, and legal penalties (Aebissa et al., 2023). As such, ensuring that employees adhere to established security protocols is a key concern for bank management. Compliance with ISPs is not merely about following rules; it's a critical component of the bank's overall security posture (Hammood et al., 2020). Effective compliance helps prevent internal and external threats, ranging from inadvertent data leaks to deliberate acts of fraud. Moreover, regulatory bodies often require strict adherence to security practices, and failure to comply can result in hefty fines and sanctions. The intention of employees to comply with ISP is a critical factor in maintaining the security and integrity of banking operations, particularly in vulnerable environments like Yemen (Al-Khulaidi et al., 2023; Central Bank of Yemen, 2022). Employee compliance is often influenced by both individual factors, such as self-efficacy and perceived response efficacy, and broader organizational factors like governance, risk management, and institutional settings. The role of governance in the banking sector has been shown to significantly affect compliance behavior, as good governance practices foster a culture of accountability and adherence to policies, including ISPs (Athari et al., 2023). In the context of Yemen, where political instability and economic uncertainty are prevalent, strong governance structures are vital in promoting employees' commitment to comply with security policies (Central Bank of Yemen, 2022). Country risk also plays a role in shaping employee behavior. Research shows that political and economic risks can indirectly affect compliance by increasing the overall uncertainty in the banking environment, making employees more cautious and inclined to follow ISPs to mitigate potential risks (Saliba et al., 2023). This is particularly relevant for the Yemeni banking sector, where the high level of political risk could heighten employees' perceptions of the importance of compliance with security protocols. Additionally, the institutional settings and regulatory frameworks within which banks operate can significantly impact employees' intentions to comply with ISPs. Studies indicate that regulatory pressures and governance structures that emphasize risk management and compliance can improve the adherence of employees to ISPs, as seen in the performance of Islamic and conventional banks (Athari et al., 2016). These findings suggest that for banks in Yemen and similar high-risk environments, creating a robust regulatory and governance framework is essential for encouraging employees to adopt compliant behaviors.

3. Model development and hypotheses

The proposed model is developed by deriving factors from PMT theory to examine the employees' intention behavior toward complying with information security policies. The PMT was developed by (Rogers, 1975), considered a well-established theory that explains the protective behaviors of humans. PMT, originally derived from expectancy-value theory, proposes that our reaction to danger is guided by two cognitive processes: threat assessment and coping assessment (Ogbanufe et al., 2023; Rogers, 1975). Moreover, threat assessment addresses the evaluation of the severity and vulnerability to harmful events, while coping assessment is a process that evaluates an individual's self-efficacy, response efficacy, and the expenditures related to the adopted response behavior (Chang et al., 2022). Protection motivation is the final result of these threat and coping assessment processes (Boss et al., 2015). It is usually defined as the behavioral intention to do the prescribed protective behavior and any subsequent protective behavior (Rogers, 1975). Within the context of information security, the PMT theory has been utilized widely, including users' reactions to computer virus threat (Tsai et al., 2016), protecting password (Vedadi and Warkentin, 2020), and organization's policies compliance by employees (Alsaad and Al-Okaily, 2022; Ogbanufe et al., 2023; Sharma and Aparicio, 2022). Fig. 1 shows the model structure that describes the relationship between the intent of employees to follow information security policies and PMT factors.

3.1. Perceived self-efficacy role towards ISP compliance

In this research, Perceived Self-Efficacy (PSE) is identified as the extent to which employees believe in their cybersecurity abilities and

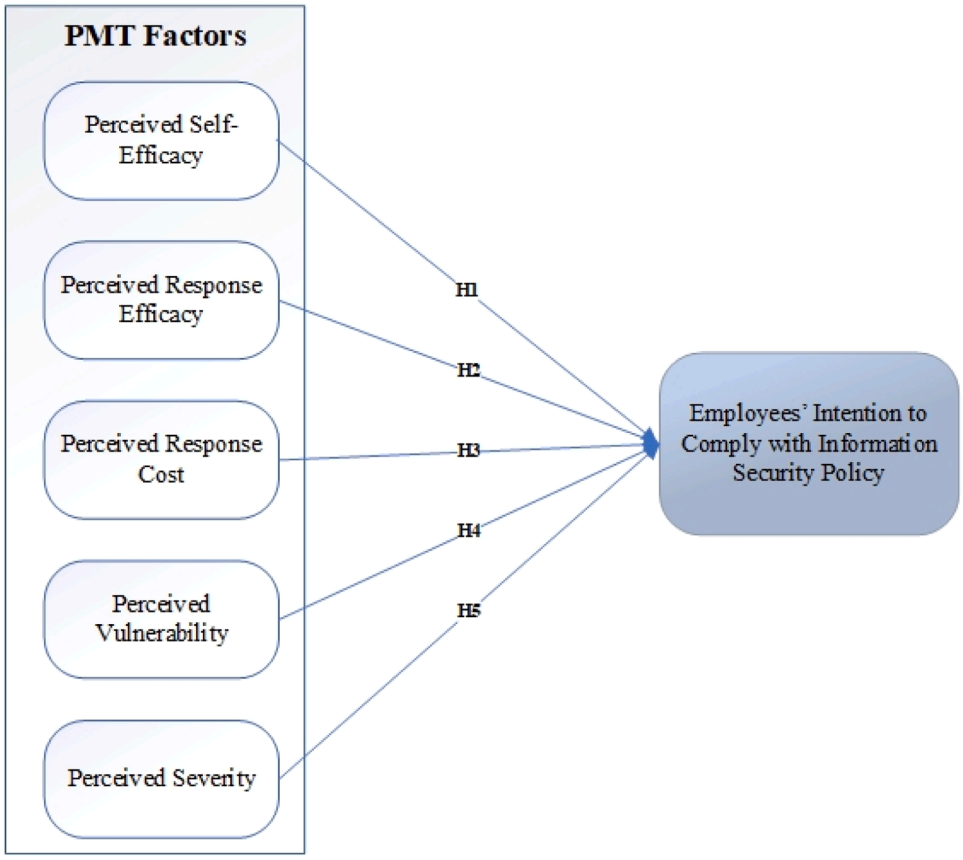

Fig. 1. Research model.

skills in dealing with cyber threats. According to previous research, PSE improves workers' ability to respond adaptively and their overall willingness to put these responses into practice (Sharma and Aparicio, 2022). Furthermore, individuals who perceive a security policy as providing substantial information about the value of their activities and the efficiency of recommended solutions in reducing the probability of information security breaches are more inclined to develop favorable intentions. This positive attitude towards the policy increases their likelihood of complying with information security measures (Alsaad and Al-Okaily, 2022). Previous research discussed the potential relationship between PSE and employees' intentions to adhere to ISP. For instance, among American working professionals, (Ogbanufe et al., 2023) reported that PSE affects security compliance behavior. Furthermore, (Alsaad and Al-Okaily, 2022) performed a research to examine the acceptance of protective technologies during the Covid-19 outbreak, when feelings of threat and fear were elevated. They found a strong correlation between self-efficacy and the development of protection motivation, which positively improved the intention to use the protection apps. Menard et al. (2017) mentioned that PSE increases the employee's perception that he or she have the necessary skills and competencies to take adaptive actions and reduce a perceived IS threats by adhering to the organization's IS policy. Thus, when an employee's PSE improves, their propensity to adopt suitable IS compliance coping strategies and behavioural intent to adhere to IS regulations and protect corporate data improve (Wong et al., 2022). Results were also validated in the USA by Torten et al. (2018), who found that PSE has significant effects on desktop security behavior among IT professionals. Zhu et al. (2022) found that PSE positively influences consumers' attitudes, which in turn impact positively on consumers' intention to participate in food risk communication in China. These discussions indicate that there is a favorable correlation between PSE and the intention of employees to comply with the ISP. Thus, this research proposes the following hypothesis:

H1: "PSE will positively affect employee's intention to comply with ISP.

3.2. *Perceived response efficacy role towards ISP compliance*

Another component of the coping assessments is the people's confidence in the efficacy of carrying out a protective coping activity, which is known as perceived Response Efficacy (PRE) (Boss et al., 2015). Individuals who hold the belief that engaging in coping behavior would provide them protection are more likely to actually do that action. Multiple studies have shown this to be valid with various security (Fan et al., 2022; Mou et al., 2022; Ogbanufe et al., 2023; Sharma and Aparicio, 2022). For instance, (Fan et al., 2022) found that there is a strong correlation between protection motivation factors like response efficacy and consumers' behavioral intention to accommodation expenditure during a pandemic. Similarly, it was shown by (Sharma and Aparicio, 2022) PRE and PSE significantly and positively affect the behavioral intention of IT workers to comply with information security regulations. Alsaad and Al-Okaily (2022) found that a high level of PRE of exposure detection apps positively contributed to enhancing the protection motivation and then positively enhanced the intention to use the apps in Jordan. Wong et al. (2022) found that PRE has a positive influence on employee's cybersecurity compliance between employees at the executive level and above in Malaysia. The study of Zhu et al. (2022) found that PRE positively influences on consumers' attitudes, which in turn impact positively on consumers' intention to participate in food risk communication in China. Neisi et al. (2020) found that PRE has a significant relationship with IS compliance intention between farmers in Iran. Torten et al. (2018) found that PRE has significant effects on desktop security behavior among IT professionals. Tsai et al. (2016) found that PRE significantly influences security compliance intention

between users of Amazon Mechanical Turk (MTurk). Therefore, the analysis shows a positive correlation between PRE and employees' intention toward information security policy compliance behavior. Consequently, the study hypothesizes the following:

H2: PRE will have a positive effect on employee's intention to comply with ISP.

3.3. Perceived response cost role towards ISP compliance

Perceived Response Cost (PRC) is the last component of the coping assessments, and it refers to the time, effort, and financial cost that individuals spend when they perform the protective coping activity (Boss et al., 2015). The likelihood of compliance with a security policy decreases as the time or effort required increases (Ogbanufe et al., 2023), similar to how people's motivation to engage in coping response behavior decreases as the cost increases. (Rajab and Eydgahi (2019) stated that when the cost and efforts of implementing recommended IS policy measures exceeds the benefits of not applying them; they are less likely to do security protections. Moreover, if employees lack the knowledge of obtaining security protections, they are unlikely to implement them. Tsai et al. (2016) state that if the using security protections are too much time, or may cause problems to other programs; they are less likely to use it. There has been prior discussion of the negative correlation between the PRC and employees' intent to adhere to information security regulations. Notably, there is a lack of consistency in the findings from the literature when it comes to this connection. For instance (Ogbanufe et al., 2023) discovered that among American professionals, the PRC had a significant negative impact on security compliance behavior. Conversely, a strong and favorable relationship was found between PRC and consumers' behavioral intention (Fan et al., 2022). Also, (Zhu et al., 2022) showed no significant influence between the PRC and consumers' attitudes and intentions toward risk communication. Furthermore Sharma and Aparicio (2022) found that PRC has not any influence on behavioural intention to protect information between IT employees in the USA. Aslo Neisi et al. (2020) found that response cost has no significant relationship with IS compliance intention in Iran. Menard et al. (2017) also found that PRC has no impact on behavioural intention to engage in voluntary secure behaviours between employees in the USA. From this, we may conclude that PRC negatively correlates with employees' intent to comply with ISP. Hence, this study proposes the following hypothesis:

H3: PRC will have a negative effect on employee's intention to comply with ISP.

3.4. Perceived vulnerability role towards ISP compliance

Perceived Vulnerability (PV) is one of the factors of the threat assessment process in PMT theory, which is defined as how vulnerable an individual feels about the danger that has been conveyed (Boss et al., 2015; Haag et al., 2021). An individual's level of compliance with the organization's security policy is influenced by their judgment of the chance that their actions might cause an information security hazard to the organization. When employees feel their organisation's information systems as being very vulnerable, they are more likely to adopt protective measures (Alghamdi, 2021; Zhu et al., 2022). There is evidence in the literature that shows a positive correlation between PV and employees' intentions to follow information security policies (Ogbanufe et al., 2023); Wong et al. (2022). For example, (Wong et al., 2022) that among Malaysian employees at the senior level and above, PV positively affects their compliance with cybersecurity. Also Sharma and Aparicio (2022) found that PV has a positive and significant impact on the behavioural intention to comply with IS policies in the USA. Fan et al. (2022) also found that consumers' behavioural intention is significantly impacted by PV in the USA. Zhu et al. (2022) found that PV is positively influence on consumer's attitude, which in turn impact positively on consumers' intention to participate in food risk communication in China. These considerations suggest a positive relationship between PV and the intention of employees toward complying with the ISP. Consequently, the study hypothesizes the following:

H4: PV will have a positive effect on employee's intention to comply with ISP.

3.5. Perceived severity role towards ISP compliance

Typically, if individuals feel a threat, they usually alter their actions based on the level of danger and decide whether or not they are willing to tolerate the threat. In that, Perceived Severity (PS) refers to the employee's assessment of the severity of the danger linked to revealing confidential information to others (Chang et al., 2022). Li et al. (2019). Additionally, (Boss et al., 2015), suggest that seeing the possible data loss as a significant threat would likely drive individuals to participate actively in security compliance measures. Consequently, an individual with a high perception of the threat's consequences will feel more fear than one with a low perception of the threat's severity, and this fear will drive that individual's IS compliance behaviour (Ogbanufe et al., 2023). Put differently, employees will be more eager to comply with IS policy if their assessments of the likelihood that danger would result in undesirable repercussions drive them (Chang et al., 2022). Past research has examined the correlation between PS and employees' intent to adhere to information security regulations (AlGhamdi et al., 2022; Ogbanufe et al., 2023; Sharma and Aparicio, 2022). For instance, (AlGhamdi et al., 2022), showed that the PSF factor positively influences employees' intent toward complying with the organization's security regulations. These discussions indicate a positive relationship between PS and employees' intention to comply with ISP. Thus, the study hypothesizes the following:

H5: PS will have a positive effect on employee's intention to comply with ISP.

4. Research methodology

4.1. Research instrument

The research was developed by extracting relevant items from prior studies on PMT and ISP compliance. Each construct in the study, such PSE, PRE, PRC, PV, PS, and employees' intention to comply with ISP, was measured using multiple items derived from established literature. These constructs were critical in capturing the different aspects of employee behavior toward ISP compliance. For example, items for PSE focused on assessing the employee's confidence in handling cyber threats, while PRE items evaluated their belief in the effectiveness of security measures. Participants rated their responses on a 5-point Likert scale, with options ranging from "1 - Strongly disagree" to "5 - Strongly agree." This Likert scale approach, widely used in similar research, provided a standardized method for measuring the intensity of participants' attitudes toward ISP compliance. The reliability of the instrument was confirmed through Cronbach's alpha, ensuring that the items were consistent in measuring their respective constructs. Table 1 in the study

Table 1
Constructs and measures of study.

Variables	No. of items	Ref.
PSE	6	(Li et al., 2019; Rajab and Eydgahi, 2019)
PRE	6	(Li et al., 2019; Tsai et al., 2016)
PRC	5	(Rajab and Eydgahi, 2019; Tsai et al., 2016)
PV	7	(Rajab and Eydgahi, 2019)
PS	5	(Boss et al., 2015; Li et al., 2019)
Intention to Comply with ISP	7	(Tsai et al., 2016)

outlines the specific sources for each construct, further reinforcing the credibility of the research instrument.

4.2. Sampling method and data collection

This study aimed to investigate the factors influencing employees' intention to comply with ISP within Yemen's banking sector. The study participants were bank employees, representing the frontline of information security management in financial institutions. To collect data, we employed an online survey distributed via Google Forms. The survey link was shared with employees across various banks in Yemen, allowing for convenient and broad data collection. A total of 210 completed questionnaires were gathered and validated for the analysis. The online format provided the flexibility to reach a larger group of participants despite potential geographical limitations.

For analyzing the collected data, the study utilized Partial Least Squares Structural Equation Modeling (PLS-SEM) using SmartPLS 4, which is particularly effective for examining complex relationships between variables and testing theoretical models. The PLS-SEM approach involves a two-stage process. The first stage is the measurement model (or "outer model"), which evaluates the reliability and validity of the constructs, ensuring that each construct accurately represents the theoretical concept it is intended to measure. The second stage is the structural model (or "inner model"), which examines the hypothesized relationships between the constructs and their influence on the employees' intention to comply with ISP. This method allows both the measurement and structural models to be analyzed simultaneously, providing comprehensive insights into the factors affecting compliance behavior. The use of bootstrapping further enhances the robustness of the findings by testing the statistical significance of the model's relationships.

5. Results

5.1. Descriptive analysis

The participants of this study were bank employees working in the Yemeni banking sector, with a total of 210 participants. The demographic characteristics of the participants are visually summarized in Fig. 1, which combines the gender distribution, age distribution, and knowledge levels in security and privacy. This consolidated figure provides a comprehensive overview of the study sample's key descriptive attributes. The gender distribution within the sample is prominently represented, showing that 77.6 % of the participants were female and 22.4 % were male. This distribution underscores the predominance of female employees in the surveyed group. The age distribution highlights that 40 % of the participants were aged 25–35 years, with the remaining 60 % belonging to other age groups, showcasing a diverse age profile. The knowledge levels in security and privacy among the participants reveal that 18.1 % identified themselves as beginners, 37.6 % as intermediate, and 6.7 % as experts. The remaining participants fell into unspecified categories, reflecting a varied range of knowledge within the study group (Fig. 2).

5.2. Assessment of the measurement model

The measurement model establishes the correlation between the constructs and their corresponding indicators (Henseler et al., 2015; Sarstedt et al., 2021). This research followed the procedures proposed by (Hair Jr. et al., 2023) for assessing the measurement model's internal consistency, reliability, and convergent validity. Composite reliability (CR) and Cronbach's alpha (CA) were utilized in this study for evaluation. Convergent validity was determined through the average variance extracted (AVE) and factor loadings. Additionally, Discriminant validity was assessed using the Heterotrait-Monotrait Ratio of correlations (HTMT), as described by (Henseler et al., 2015).

As a result, all of the CR and CA values were higher than the threshold of 0.7, as shown in Table 2 (Hair Jr. et al., 2023). Thus, the findings demonstrate that the items employed to reflect the constructs are reliable. In addition, Table 2 shows that all the model constructs have an AVE higher than 0.5, indicating convergent validity (Hair Jr. et al., 2023). Furthermore, the factor loadings for all indicators, as shown in Table 2, are above the 0.70 threshold, except for PRC3 and PV7, which have values of 0.699 and 0.677, respectively. According to (Hair Jr. et al., 2023), an item can be removed only if the factor loading value is below the threshold of 0.708 and results in a low AVE value. Consequently, the indicators PRC3 and PV7 are kept in the model since all the constructs have AVE values higher than 0.50. Thus, the findings demonstrate that the convergent validity is proven.

Regarding discriminant validity, all the HTMT values were lower than the threshold value of 0.85, as shown in Table 3. Accordingly, no issues were found with discriminant validity (Henseler et al., 2015; Sarstedt et al., 2021).

5.3. Assessment of the structural model

As the measurement model was validated, the next step in evaluating a research model is to verify its structural validity (Al-Emran et al., 2019; Hair Jr. et al., 2023). Several factors must be taken into account in order to evaluate the structural model. Structural equation modelling (SEM) is used to estimate the structural model through calculating the determination coefficient (R^2) (Cohen, 2013), path-coefficients (B-values), t-values, and p-values. To achieve this, bootstrapping is used along with one-tailed tests at a 5 % significance level, as recommended by (Hair Jr. et al., 2023). Standardized path coefficients fall within the range of −1 to + 1. The computed path coefficients near (+1) indicate robust positive correlations, whereas negative values indicate the opposite (Al-Emran et al., 2019; Hair Jr. et al., 2023).

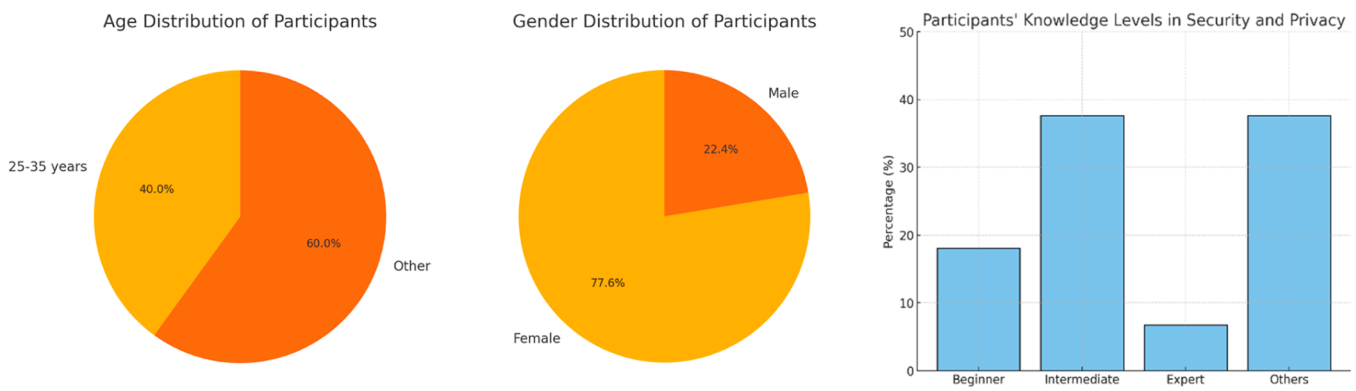

Fig. 2. Of participants.

Table 2
Reliability and convergent validity.

Constructs	Items	Factor loadings	Cronbach's alpha	Composite reliability	AVE
comply with Information Security policy	INT1	0.848	0.918	0.919	0.670
	INT2	0.818			
	INT3	0.756			
	INT4	0.838			
	INT5	0.815			
	INT6	0.811			
	INT7	0.842			
Perceived Response Cost	PRC1	0.871	0.881	0.942	0.657
	PRC2	0.910			
	PRC3	0.699			
	PRC4	0.800			
	PRC5	0.755			
Perceived Response Efficacy	PRE1	0.856	0.930	0.931	0.742
	PRE2	0.866			
	PRE3	0.879			
	PRE4	0.874			
	PRE5	0.877			
	PRE6	0.816			
Perceived Self-Efficacy	PSE1	0.870	0.920	0.926	0.713
	PSE2	0.872			
	PSE3	0.880			
	PSE4	0.838			
	PSE5	0.786			
	PSE6	0.817			
Perceived Severity	PSF1	0.728	0.851	0.857	0.627
	PSF2	0.797			
	PSF3	0.836			
	PSF4	0.782			
	PSF5	0.811			
Perceived Vulnerability	PV1	0.773	0.872	0.875	0.566
	PV2	0.773			
	PV3	0.753			
	PV4	0.798			
	PV5	0.751			
	PV6	0.734			
	PV7	0.677			

Table 3
HTMT results.

	1	2	3	4	5	6
PRC						
PRE	0.186					
PSE	0.313	0.660				
PS	0.233	0.802	0.552			
PV	0.284	0.813	0.634	0.837		
comply with Information Security policy	0.186	0.810	0.639	0.881	0.798	

The findings of the structural model are shown in Table 4. The findings indicate that the model describes 71.5 % of the variation in the employees' intent toward information security policy compliance. In addition, Prior to calculating the route coefficient, (Hair Jr. et al., 2021) suggest performing a collinearity test. Table 4 demonstrates that the model did not have any issues with collinearity since every connection had Variance Inflation Factor (VIF) values below five. The perceived self-efficacy with $\beta = 0.152$ at t-value $= 2.732$ and the perceived response efficacy with $\beta = 0.245$ at t-value $= 3.129$ exhibited a positive correlation with employees' intent toward information security policies compliance; therefore, H1 and H2 are supported. Furthermore, the perceived severity, and threat appraisal factor, with $\beta = 0.443$ at t-value $= 5.171$, has a positive relationship with the intention of employees toward complying with information security policies. Hence, the fifth hypothesis was supported. On the other hand, perceived response cost H3 ($\beta = -0.040$, $t = 1.218$) and perceived vulnerability H4 ($\beta = 0.140$, $t = 1.893$) were not supported.

In addition, the study assessed the effect size (f^2) according to the standards established by (Cohen, 2013; Hair Jr. et al., 2021). Effect sizes were classified as follows: small (0.02), medium (0.15), and large (0.35). As a result, Table 4 indicates that the impact sizes vary from small to large. Nevertheless, the perceived response cost has no significant effect on employees' intent to follow information security regulations.

6. Discussion

This research is primarily focused on providing a model based on PMT theory to assess the intention behavior of employees toward information security policies compliance. According to this study's results, PMT was found to be a suitable explanation for employees' intent toward compliance with information security policies in the banking sector. As mentioned, PMT comprises two cognitive actions: coping and threat assessment. Regarding coping factors, the results indicated a significant relationship between perceived self-efficacy and employees' behavioral intention toward information security policy compliance. These findings align with the results outlined in other research studies (Ahmad et al., 2019; Alsaad and Al-Okaily, 2022; Sharma and Aparicio, 2022). This suggests that employees in the Yemeni banking sector are more likely to have a strong desire to comply with the regulations if they think they are competent of doing so. In this regard, the results stress the need to boost employees' self-efficacy to raise their commitment to security policies. In addition, this study showed a significant correlation between perceived response efficacy and employees' intent toward compliance with information security policies. Prior studies showed similar results (Fan et al., 2022; Mou et al., 2022; Ogbanufe et al., 2023; Sharma and Aparicio, 2022; Zhu et al., 2022), which indicated that the perceived response efficacy significantly affects individuals' intention behavior. This significant relationship indicates that employees in Yemen's banking sector are more likely to adhere to information security policies if they feel confident in the efficacy of the suggested measures. No significant impact of perceived response cost on compliance intentions was found, which diverges from some previous studies (Menard et al., 2017; Neisi et al., 2020; Ogbanufe et al., 2023; Zhu et al., 2022). However, this result aligns with studies by Menard et al. (2017) and Neisi et al. (2020), which found no significant relationship between response cost and behavioral intentions, particularly in cases where the costs are perceived to be minimal or manageable. According to this result, it is suggested that the perceived costs, such as time, money, and effort, do not greatly deter the bank employees in Yemen. Thus, these costs are not impacting the employees' intention to comply with information security policies.

On the other hand, the two threat assessment factors showed different results. For example, this study hypothesized that perceived vulnerability significantly influences employees' behavioral intentions. However, this hypothesis was not supported. This finding contradicts

Table 4
Structural model results.

Hypotheses	Path	B	T value	P values	f^2	R^2	VIF
H1	Perceived Self-Efficacy -> comply with Information Security policy	0.152	2.732	0.006	0.045	0.715	1.775
H2	Perceived Response Efficacy -> comply with Information Security policy	0.245	3.129	0.002	0.073		2.909
H3	Perceived Response Cost -> comply with Information Security policy	−0.040	1.218	0.223	0.005		1.122
H4	Perceived Vulnerability -> comply with Information Security policy	0.140	1.893	0.058	0.024		2.851
H5	Perceived Severity -> comply with Information Security policy	0.443	5.171	0.000	0.273		2.505

previous research conducted by (Wong et al., 2022) and (Ifinedo, 2012), showing a substantial impact of perceived vulnerability on individuals' behavior. However, this result aligns with the research conducted by (Alghamdi, 2021), which investigated the influence of cybersecurity knowledge on employee behavior. Their findings indicated that the impression of vulnerability did not substantially impact workers' behavior, particularly regarding their recognition of cyberattack risks (Alghamdi, 2021). Given the absence of a statistically significant relationship in this study, it can be concluded that the beliefs held by employees in the Yemeni banking sector about their susceptibility to security threats do not significantly impact their desire to adhere to information security policies. The potential causes of this discrepancy may stem from insufficient knowledge of the organization's particular security concerns or because their perception of their vulnerability is at odds with the risks addressed in the policies. In addition, this study hypothesized that perceived severity significantly impacts employees' behavioral intentions. The results showed that this hypothesis was supported and consistent with previous research studies (Chang et al., 2022; Fan et al., 2022). The study results indicate a growing inclination among bank workers in Yemen to adhere to information security regulations. This is because workers comprehend the seriousness of the consequences associated with not adhering to the regulations.

7. Conclusions

This study examined the factors influencing employees' compliance with information security policies in the Yemeni banking sector, utilizing Protection Motivation Theory (PMT) as the theoretical framework. The results demonstrated that perceived self-efficacy, response efficacy, and severity significantly affect employees' intentions to comply with information security policies. This underscores the importance of employees' confidence in their abilities and the perceived effectiveness of protective measures. However, perceived response cost and vulnerability did not have significant effects, suggesting that these factors may not deter compliance in the Yemeni context.

The study contributes to the literature by applying PMT in a developing country facing unique challenges, offering practical implications for enhancing information security compliance in similar contexts. Future research should consider integrating other behavioral theories and expanding the sample size to gain further insights into employee behavior regarding information security.

7.1. Theoretical implications

This study presents several theoretical contributions. The model is constructed from the PMT theory, which is widely recognized as one of the most often-referenced theories in security behavior. Previous studies have confirmed the theory's applicability in several domains (Lin and Chang, 2023; Tsai et al., 2016). However, validating the proposed model in the banking industry, specifically in a developing country like Yemen, is a new aspect that has not been investigated in the current literature. Consequently, it is expected that this study will support the validation of the PMT theory in other organizational domains. Secondly, the study contributed to the current understanding of the factors impacting compliance behavior toward information security policies at the individual level. The innovation and contribution of the research are indeed clear, particularly when considering its specific focus on the Yemeni banking sector. While much of the existing literature on PMT and ISP compliance has been conducted in developed countries or in different sectors, this research provides a unique and valuable contribution by applying the PMT framework in a developing country context, which is notably underrepresented in the literature.

7.2. Practical implications

This study provides insights into the factors that influence employees' behavioral intention toward complying with information security policies by using the PMT framework. Consequently, the findings of this research have multiple practical implications. Considering the significance of perceived self-efficacy and perceived response efficacy in influencing an individual's intention toward compliance with information security policies, it would be beneficial for management to expose the employees to new security technologies and motivate them to acquire the essential skills and knowledge to safeguard the organization's information system assets. Following information security regulations and instructions will be easier if such encouragements are available for control and skill development. Similarly, bank leaders should make their staff aware of the dangers posed by the exploitation, misuse, and destruction of information systems. Additionally, consistent communication, training, and support from bank committees may underscore the significance of complying with information security regulations.

7.3. Policy implications

The findings of this study provide valuable insights for practitioners and policymakers in the Yemeni banking sector and beyond, offering actionable strategies to enhance information security policy compliance. Policymakers should prioritize developing and implementing national cybersecurity frameworks tailored to the unique challenges of developing nations. These frameworks should include standardized security protocols, clear compliance guidelines, and practical tools that banks can adopt with minimal resource strain. Collaborative efforts among government agencies, industry leaders, and international organizations are essential to enhance the sector's overall cybersecurity posture. Initiatives such as joint training programs, information-sharing platforms, and coordinated responses to cyber threats can build a unified defense against evolving risks. Furthermore, Investment in capacity-building initiatives is crucial to address the shortage of skilled personnel in the field of information security. Policymakers can establish scholarship programs, training centers, or public-private partnerships to nurture local talent and ensure a steady pipeline of cybersecurity professionals. Finally, addressing the economic barriers to compliance should also be a priority. Governments and regulatory bodies could consider offering banks financial incentives, subsidies, or grants for adopting advanced security measures and conducting regular employee training.

7.4. Study limitations and future research

The study presents some limitations that warrant further investigation by future research, although it does provide substantial theoretical and practical contributions to the current knowledge of workers' information security compliance behavior. The initial limitation is that the PMT theoretical framework is the only one used to determine behavioral aspects. It may be helpful to incorporate other behavioral theories to further understand what influences workers' compliance behavior in information security. In addition, 210 replies were used to create the sample. The study's design and analysis were suitable for the PLS method. However, a bigger sample size might achieve further statistical power and performance. Furthermore, while the study focused on the core constructs of PMT, it did not include mediating variables such as fear. Although previous studies have indicated the potential significance of these variables, they were excluded to maintain the study's focus on validating the PMT framework in the specific context of the Yemeni banking sector. Future research could examine how these factors influence the relationship between PMT components and compliance behavior, offering a more comprehensive understanding of the factors at play. Additionally, this study did not assess the influence of moderating variables, such as gender, age, organizational culture, or leadership style on the relationship between PMT factors and the intention of employees toward complying with information security policies. Thus, exploring this area in future research could yield valuable insights and might

improve the robustness of the model.

Funding acknowledgement

This research is funded by the Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah. This study is a part of the research conducted and funded by University Postgraduate Research Grant (PGRS230398).

Ethical statement

This study was conducted in accordance with the ethical standards of UMPSA and adhered to all applicable guidelines for research involving human participants. Informed consent was obtained from all participants, and their anonymity and confidentiality were strictly maintained.

CRediT authorship contribution statement

Ebrahim Mohammed Alrawhani: Writing – original draft, Methodology, Data curation, Conceptualization. **Awanis Romli:** Writing – review & editing, Supervision, Resources, Funding acquisition. **Mohammed A. Al-Sharafi:** Writing – review & editing, Supervision, Formal analysis, Conceptualization.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Abdualmajed, A.G., AlkhulaidI, A.A., Nada, K.A., Moneer, A.S., Mijahed, A., Nesmah, A., 2022. Information security gap analysis: an applied study on The Yemeni banking sector's technology and innovation practices. Seybold Rep. 17 (11), 106–132. https://doi.org/10.5281/zenodo.7307870.

Aebissa, B., Dhillon, G., Meshesha, M., 2023. The direct and indirect effect of organizational justice on employee intention to comply with information security policy: the case of Ethiopian banks. Comput. Secur. 130, 103248.

Ahmad, Z., Ong, T.S., Liew, T.H., Norhashim, M., 2019. Security monitoring and information security assurance behaviour among employees: an empirical analysis. Inf. Comput. Secur. 27 (2), 165–188. https://doi.org/10.1108/ICS-10-2017-0073.

Akello, B.O., 2024. Organizational information security threats: Status and challenges. World J. Adv. Eng. Technol. Sci. 11 (1), 148–162.

Al-Emran, M., Al-Qaysi, N., Al-Sharafi, M.A., Khoshkam, M., Foroughi, B., Ghobakhloo, M., 2025. Role of perceived threats and knowledge management in shaping generative AI use in education and its impact on social sustainability. Int. J. Manag. Educ. 23 (1), 101105. https://doi.org/10.1016/j.ijme.2024.101105.

Al-Emran, M., Al-Sharafi, M.A., Foroughi, B., Iranmanesh, M., Alsharida, R.A., Al-Qaysi, N., Ali, N.A., 2024. Evaluating the barriers affecting cybersecurity behavior in the Metaverse using PLS-SEM and fuzzy sets (fsQCA). Comput. Hum. Behav. 159, 108315. https://doi.org/10.1016/j.chb.2024.108315.

Al-Emran, M., Mezhuyev, V., & Kamaludin, A. (2019). PLS-SEM in information systems research: a comprehensive methodological reference. Proceedings of the International Conference on Advanced Intelligent Systems and Informatics 2018 4.

Alghamdi, M.I., 2021. Determining the impact of cyber security awareness on employee behaviour: a case of Saudi Arabia. Mater. Today.: Proc. https://doi.org/10.1016/j.matpr.2021.04.093.

AlGhamdi, S., Win, K.T., Vlahu-Gjorgievska, E., 2022. Employees' intentions toward complying with information security controls in Saudi Arabia's public organisations. Gov. Inf. Q. 39 (4), 101721. https://doi.org/10.1016/j.giq.2022.101721.

Alkhudhayr, F., Alfarraj, S., Aljameeli, B., & Elkhdiri, S. 2019. Information security: A review of information security issues and techniques. 2019 2nd international conference on computer applications & information security (ICCAIS).

Al-Khulaidi, A., Al-Ashwal, M., Nasser, A., Al-Ansi, N., 2023. Information security risk management in Yemeni banks: an evaluation of current practices. Int. J. Eng. Trends Technol. 71, 225–237. https://doi.org/10.14445/22315381/IJETT-V71I4P220.

Al-Momani, A.A.M., Ramayah, T., Al-Sharafi, M.A., 2024. Exploring the impact of cybersecurity on using electronic health records and their performance among healthcare professionals: a multi-analytical SEM-ANN approach. Technol. Soc. 77, 102592. https://doi.org/10.1016/j.techsoc.2024.102592.

Alsaad, A., Al-Okaily, M., 2022. Acceptance of protection technology in a time of fear: the case of Covid-19 exposure detection apps. Inf. Technol. People 35 (3), 1116–1135. https://doi.org/10.1108/ITP-10-2020-0719.

Al-Sharafi, M.A., Arshah, R.A., Alajmi, Q., Herzallah AT, F., & Qasem, Y.A. 2018. The Influence of Perceived Trust on Understanding Banks' Customers behavior to Accept Internet Banking Services.

Alzamil, Z.A., 2018. Information security practice in Saudi Arabia: case study on Saudi organizations. Inf. Comput. Secur. 26 (5), 568–583. https://doi.org/10.1108/ICS-01-2018-0006.

Amankwa, E., Loock, M., Kritzinger, E., 2022. The determinants of an information security policy compliance culture in organisations: the combined effects of organisational and behavioural factors (ahead-of-print(ahead-of-print)). Inf. Comput. Secur.. https://doi.org/10.1108/ICS-10-2021-0169.

Athari, S.A., Adaoglu, C., Bektas, E., 2016. Investor protection and dividend policy: the case of Islamic and conventional banks. Emerg. Mark. Rev. 27, 100–117.

Athari, S.A., Saliba, C., Khalife, D., Salameh-Ayanian, M., 2023. The role of country governance in achieving the banking sector's sustainability in vulnerable environments: new insight from emerging economies. Sustainability 15 (13), 10538.

Bany Mohammad, A., Al-Okaily, M., Al-Majali, M., Masa'deh, R.E., 2022. Business Intelligence and Analytics (BIA) usage in the banking industry sector: an application of the TOE framework. J. Open Innov.: Technol. Mark. Complex. 8 (4), 189. https://doi.org/10.3390/joitmc8040189.

Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D., Polak, P., 2015. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. MIS Q.: Manag. Inf. Syst. 39 (4), 1–72. https://doi.org/10.25300/MISQ/2015/39.4.5.

Central Bank of Yemen. 2022. Cybersecurity in the Banking Sector in Yemen. ⟨https://www.centralbank.gov.ye/Home/index⟩.

Chang, H.H., Wong, K.H., Lee, H.C., 2022. Peer privacy protection motivation and action on social networking sites: privacy self-efficacy and information security as moderators. Electron. Commer. Res. Appl. 54, 101176. https://doi.org/10.1016/j.elerap.2022.101176.

Cohen, J., 2013. Statistical power analysis for the behavioral sciences. Academic press.

Fan, A., Kline, S.F., Liu, Y., Byrd, K., 2022. Consumers' lodging intentions during a pandemic: empirical insights for crisis management practices based on protection motivation theory and expectancy theory. Int. J. Contemp. Hosp. Manag. 34 (4), 1290–1311. https://doi.org/10.1108/IJCHM-07-2021-0889.

Gaurav, A., Panigrahi, P.K., 2022. Analysis of security paradigms for resource and infrastructure management in global organizations. J. Glob. Inf. Manag. (JGIM) 31 (2), 1–11.

Gwebu, K., Wang, J., Hu, M., 2020. Information security policy noncompliance: an integrative social influence model. Inf. Syst. J. 30 (2), 220–269.

Haag, S., Siponen, M., Liu, F., 2021. Protection motivation theory in information systems security research: a review of the past and a road map for the future. ACM SIGMIS Database.: Database. Adv. Inf. Syst. 52 (2), 25–67.

Hair Jr, J.F., Hult, G.T.M., Ringle, C.M., & Sarstedt, M. (2021). A primer on partial least squares structural equation modeling (PLS-SEM). Sage publications.

Hair Jr, J., Hair Jr, J.F., Sarstedt, M., Ringle, C.M., & Gudergan, S.P. 2023. Advanced issues in partial least squares structural equation modeling. saGe publications.

Hammood, W.A., Abdullah, R., Hammood, O.A., Mohamad Asmara, S., Al-Sharafi, M.A., Muttaleb Hasan, A., 2020. A review of user authentication model for online banking system based on mobile IMEI number. IOP Conf. Ser.: Mater. Sci. Eng. 769 (1), 012061. https://doi.org/10.1088/1757-899x/769/1/012061.

Henseler, J., Ringle, C.M., Sarstedt, M., 2015. A new criterion for assessing discriminant validity in variance-based structural equation modeling. J. Acad. Mark. Sci. 43, 115–135.

Hu, S., Hsu, C., Zhou, Z., 2021. The impact of SETA event attributes on employees' security-related Intentions: an event system theory perspective. Comput. Secur. 109, 102404. https://doi.org/10.1016/j.cose.2021.102404.

Ifinedo, P., 2012. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comput. Secur. 31 (1), 83–95.

Khando, K., Gao, S., Islam, S.M., Salman, A., 2021. Enhancing employees information security awareness in private and public organisations: a systematic literature review. Comput. Secur. 106, 102267.

Koolen, C., Wuyts, K., Joosen, W., Valcke, P., 2024. From insight to compliance: appropriate technical and organisational security measures through the lens of cybersecurity maturity models. Comput. Law Secur. Rev. 52, 105914.

Kuzior, A., Arefieva, O., Vovk, O., Brożek, P., 2022. Innovative development of circular systems while ensuring economic security in the industry. J. Open Innov.: Technol., Mark., Complex. 8 (3), 139. https://doi.org/10.3390/joitmc8030139.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., Yuan, X., 2019. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. Int. J. Inf. Manag. 45, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017.

Lin, H.-X., Chang, C., 2023. Factors associated with the quitting intention among Chinese adults: application of protection motivation theory. Curr. Psychol. 42 (2), 1083–1091.

Makeri, Y.A., 2020. The strategy detection on information security in corporate organizations on crucial asset. JOIV: Int. J. Inform. Vis. 4 (1), 35–39.

Matkovskaya, Y.S., Vechkinzova, E., Biryukov, V., 2022. Banking ecosystems: identification latent innovation opportunities increasing their long-term competitiveness based on a model the technological increment. J. Open Innov.: Technol. Mark. Complex. 8 (3), 143. https://doi.org/10.3390/joitmc8030143.

Menard, P., Bott, G.J., Crossler, R.E., 2017. User motivations in protecting information security: protection motivation theory versus self-determination theory. J. Manag. Inf. Syst. 34 (4), 1203–1230. https://doi.org/10.1080/07421222.2017.1394083.

Mou, J., Cohen, J.F., Bhattacherjee, A., Kim, J., 2022. A test of protection motivation theory in the information security literature: a meta-analytic structural equation modeling approach. J. Assoc. Inf. Syst. 23 (1), 196–236.

Nasir, A., Abdullah Arshah, R., Ab Hamid, M.R., 2019. A dimension-based information security culture model and its relationship with employees' security behavior: a case study in Malaysian higher educational institutions. Inform. Secur. J.: A Global Perspect. 28 (3), 55–80.

Nasser, A., Kh, N., Alsharabi, N., 2020. On the standardization practices of the information security operations in banking sector: evidence from Yemen. Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol. 8, 8–18.

Neisi, M., Bijani, M., Abbasi, E., Mahmoudi, H., Azadi, H., 2020. Analyzing farmers' drought risk management behavior: evidence from Iran. J. Hydrol. 590, 125243. https://doi.org/10.1016/j.jhydrol.2020.125243.

Ogbanufe, O., Crossler, R.E., Biros, D., 2023. The valued coexistence of protection motivation and stewardship in information security behaviors. Comput. Secur. 124, 102960. https://doi.org/10.1016/j.cose.2022.102960.

Qatawneh, N., 2024. Empirical insights into business intelligence adoption and decision-making performance during the digital transformation era: extending the TOE model in the Jordanian banking sector. J. Open Innov.: Technol. Mark. Complex. 10 (4), 100401. https://doi.org/10.1016/j.joitmc.2024.100401.

Rajab, M., Eydgahi, A., 2019. Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. Comput. Secur. 80, 211–223. https://doi.org/10.1016/j.cose.2018.09.016.

Rogers, R.W., 1975. A protection motivation theory of fear appeals and attitude change. J. Psychol. 19 (1), 93–114. https://doi.org/10.1080/00223980.1975.9915803.

Saliba, C., Farmanesh, P., Athari, S.A., 2023. Does country risk impact the banking sectors' non-performing loans? Evidence from BRICS emerging economies. Financ. Innov. 9 (1), 86.

Sarstedt, M., Ringle, C.M., Hair, J.F., 2021. Partial least squares structural equation modeling. Handbook of market research. Springer, pp. 587–632.

Sas, M., Reniers, G., Ponnet, K., Hardyns, W., 2021. The impact of training sessions on physical security awareness: measuring employees' knowledge, attitude and self-reported behaviour. Saf. Sci. 144, 105447. https://doi.org/10.1016/j.ssci.2021.105447.

Sharma, S., Aparicio, E., 2022. Organizational and team culture as antecedents of protection motivation among IT employees. Comput. Secur. 120, 102774. https://doi.org/10.1016/j.cose.2022.102774.

Shulha, O., Yanenkova, I., Kuzub, M., Muda, I., Nazarenko, V., 2022. Banking information resource cybersecurity system modeling. J. Open Innov.: Technol. Mark. Complex. 8 (2), 80. https://doi.org/10.3390/joitmc8020080.

Torten, R., Reaiche, C., Boyle, S., 2018. The impact of security awarness on information technology professionals' behavior. Comput. Secur. 79, 68–79. https://doi.org/10.1016/j.cose.2018.08.007.

Tsai, H.-Y.S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N.J., Cotten, S.R., 2016. Understanding online safety behaviors: a protection motivation theory perspective. Comput. Secur. 59, 138–150. https://doi.org/10.1016/j.cose.2016.02.009.

Vedadi, A., Warkentin, M., 2020. Can secure behaviors be contagious? A two-stage investigation of the influence of herd behavior on security decisions. J. Assoc. Inf. Syst. 21 (2), 3.

Wong, L.-W., Lee, V.-H., Tan, G.W.-H., Ooi, K.-B., Sohal, A., 2022. The role of cybersecurity and policy awareness in shifting employee compliance attitudes: building supply chain capabilities. Int. J. Inf. Manag. 66, 102520. https://doi.org/10.1016/j.ijinfomgt.2022.102520.

Yuryna Connolly, L., Lang, M., Gathegi, J., Tygar, D.J., 2017. Organisational culture, procedural countermeasures, and employee security behaviour. Inf. Comput. Secur. 25 (2), 118–136. https://doi.org/10.1108/ICS-03-2017-0013.

Zhu, Y., Wen, X., Chu, M., Sun, S., 2022. Consumers' intention to participate in food safety risk communication: a model integrating protection motivation theory and the theory of reasoned action. Food Control 138, 108993. https://doi.org/10.1016/j.foodcont.2022.108993.