International Journal of Safety and Security Engineering
Vol. 15, No. 3, March, 2025, pp. 443-453
Journal homepage: http://iieta.org/journals/ijsse

Determinants of Security Behavior Intention in State-Owned Enterprises: Applying Protection Motivation Theory to Phishing Emails

Okta Pratama, Riadi Arief Aladin, Budiarto Lim, Arta Moro Sundjaja*

Management Department, Binus Business School Master Program, Bina Nusantara University, Jakarta 11530, Indonesia

Corresponding Author Email: asundjaja@binus.edu

https://doi.org/10.18280/ijsse.150304

Received: 10 July 2024
Revised: 13 November 2024
Accepted: 28 December 2024
Available online: 31 March 2025

Keywords:
SOEs, extended protection motivation theory, threat awareness, security awareness

ABSTRACT

The increasing prevalence of cyber security threats underscores the need to understand employee behavior to prevent phishing-related risks and effectively promote a sustainable working environment. This issue is particularly critical for state-owned enterprises (SOEs), especially those operating in sensitive industries. Our study explores the factors influencing the behavior intentions of SOE employees to avoid clicking on phishing email links. The research adopts a quantitative approach, utilizing Structural Equation Modelling (SEM) for data analysis using SmartPLS 4.1.0 software. A sample size of 189 respondents was determined using the G-Power Calculator and selected through purposive sampling. The results reveal that self-efficacy, perceived vulnerability, and perceived severity significantly influence security behavior intention. Furthermore, threat awareness was identified as a significant predictor of response efficacy, perceived vulnerability, and self-efficacy. Security knowledge was found to play a crucial role in shaping perceived severity, perceived vulnerability, and response efficacy. However, three hypotheses were not supported, specifically the relationships between threat awareness and perceived severity, security awareness and self-efficacy, and response efficacy and security behavior intention. These findings underscore the need for organizations to address the gaps by reinforcing practical training and targeted intervention for strengthening employee perception of severity perception, self-efficacy, and security behavior intention. The study highlights the importance of implementing robust cybersecurity awareness campaigns and policies within organizations prone to cyber threats. By fostering a culture of vigilance and improving employees understanding of the severity and vulnerability of phishing attacks, organizations can enhance their resilience against cyber threats and mitigate potential risks effectively.

1. INTRODUCTION

Due to the rapidly changing digital landscape, cybersecurity has become a top priority for corporations worldwide, including Indonesia's state-owned enterprise (SOE) sector. Phishing, one of the many cyber hazards, has become a significant issue, leading enterprises to strengthen their defenses to protect sensitive data and critical infrastructure [1]. The utilization of this malevolent strategy has resulted in significant monetary damages, as demonstrated by the FBI's startling disclosure of a staggering sum of US $10 billion or 147 trillion Indonesian Rupiah being lost to phishing attacks in 2022 [2]. While precise data on the financial losses caused by phishing in Indonesia is not given, the widespread use of financial applications and digitalization has led to a rise in fraud cases. This has left users at risk of cybercrimes due to insufficient improvements in security systems. The Indonesian authorities have implemented cyber patrols to combat cybercrime. However, fraud continues to be widespread due to the inadequacy of fraud prevention mechanisms and the absence of comprehensive cybersecurity policies [3]. The prevalence of phishing is underscored by the significant number of reported cases, amounting to 164,131 incidents in the same year [2], highlighting both the financial consequences and the potential for identity theft and participation in more extensive fraudulent schemes.

The SOE sector, which includes banking, energy, information, communication, and technology (ICT), plays a crucial role in Indonesia's economy, with substantial revenue and profit numbers [4]. Despite its economic importance, this sector faces an increased vulnerability to phishing attacks due to its crucial function and high employee welfare standards [5]. Furthermore, the transition to remote work, accelerated by the worldwide pandemic, has emphasized the need to strengthen cybersecurity protocols for SOE staff [6]. Central Bureau of Statistics reports that around 65.78% of Indonesia's population will be involved in productive activities [7]. As a result, the risk of cyber-attacks, namely phishing attacks that target individual weaknesses, has become increasingly noticeable [8].

Previous studies have provided insight into the complex psychological and environmental elements that affect how SOEs employees respond to phishing attacks. However, these studies have produced inconsistent results. Several studies

emphasize the significant influence of perceived severity, perceived vulnerability, and self-efficacy on security behavior intentions [3, 9, 10]. However, other studies reach different conclusions [11]. Moreover, there are differing viewpoints on threat and security awareness [12]. Certain studies suggest a direct relationship between these awareness levels and engaging in self-protective actions [13, 14]. However, other research warns of potential drawbacks, such as a decreased perception of vulnerability, which may result in less stringent protective measures [10, 15].

Based on the synthesis of previous research findings, the researchers conclude that a substantial gap persists in understanding the interaction of these determinants within the context of SOEs. Their employees often operate under unique organizational and cultural frameworks that may influence their cybersecurity behaviors. Moreover, existing research has focused on the general population or private sector organizations, leaving the dynamic within SOEs, especially in the financial and non-financial sectors, largely unexplored.

This study addresses these gaps by focusing on the interplay of protection motivation theory determinants, such as perceived severity, perceived vulnerability, threat awareness, and self-efficacy. Moreover, their impact on the behavior intention of SOE employees in responding to phishing attacks is also important. This research seeks to provide nuanced insights into the factors influencing cybersecurity behavior. The findings are expected to contribute to developing interventions and strategies to foster a sustainable working environment by enhancing cybersecurity resilience in both financial and non-financial sectors of SOEs.

2. LITERATURE REVIEW

2.1 Protection motivation theory

The Protection Motivation Theory (PMT) is a conceptual framework created by Rogers in 1975 and subsequently elaborated upon in 1983. The concept of PMT, initially introduced in health behavior, seeks to understand how individuals react to risks and take preventive actions [16]. Over the years, PMT has been used in several areas, such as cybersecurity, to analyze how people respond and behave to protect themselves from possible threats of cyberattack [13, 17].

The PMT theory suggests that individuals choose protective behaviors according to their subjective assessment of potential risks. These perceptions are developed based on two promary evaluations: perceived vulnerabilty and severity. Perceived vulnerability is an individual's subjective susceptibility assessment to a specific hazard. It entails evaluating the probability of being exposed to the threat. Perceived severity refers to an indivual's evaluation of the probable repercussions or harm from a threat. The process entails assessing the severity of the anticipated consequences of a perceived danger threat [16, 18].

According to the theories, individuals are more inclined to exhibit defensive responses when they perceive a combination of high susceptibility and high magnitude of the threat. This impression elicits a drive to safeguard oneself from impending danger using precautionary measures. The PMT has played a crucial role in examining the intention of individuals to engage in secure conduct within the field of cybersecurity. Researchers can gain insights into individuals' intentions to adopt security measures and protect their digital assets by analyzing their perceptions of vulnerability and severity of cyber threats. This can be achieved by referring to studies conducted by previous studies [10, 15-18].

2.2 Extending protection motivation theory

An extension of PMT emphasizes the importance of threat and security awareness as additional factors influencing individuals' motivation to adopt protective behavior. Threat awareness refers to individuals' comprehension of cybersecurity risk and their understanding of vulnerabilities within information systems. This awareness can motivate individuals to take self-protective actions by highlighting the seriousness of potential threats [19]. However, research also indicates a paradoxical effect, where heightened awareness may reduce perceived vulnerability, leading individuals to adopt fewer comprehensive security measures [10, 15]. For instance, the previous research demonstrated that awareness of cyber risks significantly enhances government employee's ability to implement adequate cybersecurity measures [13]. Similarly, the previous research highlighted that an individual's perception of cyberattack severity influences their behavioral tendencies to avoid security risks [20].

In addition to threat awareness, security awareness is pivotal in enhancing individuals understanding of cybersecurity risks and security measures. Security awareness encompasses knowledge of cyber threats, comprehension of security strategies, and adherence to security protocols in professional and personal contexts [14]. This includes recognizing cyber threats, implementing security measures, and complying with established security regulations. Effective security education and awareness programs can significantly improve individuals understanding of their roles and responsibilities in cybersecurity. The program aims to protect valuable information and systems, mitigating the risks of cyberattacks that could disrupt operations and damage organizational reputation [21-23].

2.3 Hypothesis development

2.3.1 Threat awareness and perceived severity

Research indicates that individuals with greater awareness of cyber threats tend to perceive these threats as more severe [13]. In the context of SOEs, where sensitive data and critical infrastructure are at risk, heightened threat awareness is vital [24]. Awareness of threats like phishing enables employees to recognize risks such as operational disruptions, financial losses, and reputational damage [25]. Those issues were particularly critical in high-risk environments like SOEs. With organizational policies emphasizing cybersecurity preparedness, employees who understand these risks are more likely to perceive cyber threats as severe and adopt proactive measures to protect organizational assets [10, 26]. Therefore, the hypothesis is:

H_1: *Threat awareness positively affects perceived severity in avoiding clicking on phishing emails.*

2.3.2 Threat awareness and perceived vulnerability

Research suggests that as individuals become more informed about potential cyber threats, their perception of vulnerability to those threats increases [27]. In SOEs, where employees handle sensitive data and operate within high-risk environments, increased awareness of cybersecurity dangers

increases recognition of their susceptibility to security threats. Awareness programs, including phishing education and simulation exercises, equip employees with the necessary skills to identify and avoid phishing attempts, reinforcing their understanding of vulnerabilities [28]. Furthermore, security training and a strong organizational cybersecurity culture encourage proactive behaviors, motivating employees to adopt security measures and reduce exposure to cyber risks [13]. By recognizing their likelihood of being impacted by phishing and other cyberattacks, SOE employees develop a stronger sense of perceived vulnerability, critical for fostering preventive actions. Therefore, this led to the formulation of the following hypothesis:

H_2: *Threat awareness positively affects perceived vulnerability in avoiding clicking on phishing emails.*

2.3.3 Threat awareness and self-efficacy

Research demonstrates a positive correlation between threat awareness and self-efficacy. For example, entrepreneurs aware of ransomware threats are more confident in implementing effective self-protective measures [17]. Similarly, during the COVID-19 pandemic, merchants aware of the risks from contaminated banknotes exhibited great confidence in adopting mobile payment solutions, enhancing their motivation to continue the solutions [28]. Finally, state-owned employees face heightened cybersecurity risk, and threat awareness is crucial for building confidence in preventing phishing attacks [29]. Conversely, when individuals perceive higher risks associated with unreliable information, their self-efficacy in sharing information may decrease, given concerns about the consequences of spreading misinformation [30]. Therefore, this led to the formulation of the following hypothesis:

H_3: *Threat awareness positively affects self-efficacy in avoiding clicking on phishing emails.*

2.3.4 Threat awareness and response efficacy

Research indicates a positive relationship between threat awareness and response efficacy across various contexts. For instance, entrepreneurs with greater awareness of cybersecurity threats are more likely to trust the effectiveness of protective measures they can implement against ransomware [17]. Similarly, individuals who perceive higher risks associated with information quality are more confident that their information-sharing behaviors can mitigate these risks for themselves and others [30]. In the context of SOEs, heightened threat awareness among employees in high-risk industries can similarly strengthen their belief in the efficacy of organizational policies and protective behaviors [31]. This underscores the importance of tailored training programs and clear policy communication to enhance response efficacy [32]. Therefore, this led to the formulation of the following hypothesis:

H_4: *Threat awareness positively affects response efficacy in avoiding clicking on phishing emails.*

2.3.5 Security awareness and perceived severity

Research demonstrates a positive correlation between security awareness and perceived severity. Individuals with higher cybersecurity awareness are more likely to assess cyber threats as severe, which motivates protective behaviors [14]. For example, perceived knowledge about online risks and countermeasures heightens the awareness of cybersecurity consequences, reinforcing the sense of threat severity [10]. Similarly, users with heightened security awareness tend to recognize the severity of threats in their desktop environments, leading to proactive protective behaviors. These findings are consistent with the Protection Motivation Theory, which posits that great threat awareness and perceived severity drive individuals to adopt protective actions [18]. Therefore, this led to the formulation of the following hypothesis:

H_5: *Security awareness positively affects perceived severity in avoiding clicking on phishing emails.*

2.3.6 Security awareness and perceived vulnerability

Research indicates that increased security awareness often makes individuals perceive greater vulnerability to cybersecurity threats. Heightened awareness of data collection practices and information security risks can make individuals feel more exposed, influencing their behavior on social networks [33]. Similarly, as employees gain a deeper understanding of cybersecurity risks, they become more conscious of how these risks could personally affect them, increasing their perceived vulnerability [14]. Conversely, evidence suggests a negative association between perceived knowledge and perceived vulnerability. Individuals who believe they are highly knowledgeable about cyber threats and safety measures tend to feel less susceptible to becoming victims of cybercrime [10]. This highlights complex relationships where perceived knowledge may provide a sense of security, potentially reducing feelings of vulnerability. Therefore, this led to the formulation of the following hypothesis:

H_6: *Security awareness positively affects perceived vulnerability in avoiding clicking on phishing emails.*

2.3.7 Security awareness and self-efficacy

Research indicates that security awareness and self-efficacy influence users' security behaviors, particularly in mitigating email and website-based phishing attacks [34]. As individuals become more knowledgeable about security threats and protective measures, their confidence in effectively identifying suspicious emails or avoiding phishing links increases [35]. Additionally, coping awareness, a key security awareness component, strengthens individuals' confidence in handling cyber threats [15]. This suggests that as employees become more adapt at recognizing and managing cyber risks, their belief in their ability to implement adequate security measures is significantly enhanced. Therefore, this led to the formulation of the following hypothesis:

H_7: *Security awareness positively affects self-efficacy in avoiding clicking on phishing emails.*

2.3.8 Security awareness and response efficacy

Research shows a positive correlation between security awareness and response efficacy across various contexts. As individuals gain awareness of strategies to manage and cope with cyber threats, their confidence in the effectiveness of protective measures increases [15]. This heightened understanding strengthens their belief in the efficacy of protective actions across different cyber threats. Additionally, individuals who perceive themselves as well-informed about cyber risks and security measures tend to have greater confidence in the success of their actions [10]. Awareness of information security threats further reinforces belief in the effectiveness of recommended responses [18]. Consequently, as security awareness grows, so does the belief that proactive measures can effectively prevent or mitigate security threats

[13]. Therefore, this led to the formulation of the following hypothesis:

H8: *Security awareness is a positive predictor for response efficacy in avoiding clicking on phishing emails.*

2.3.9 Perceived severity and security behavior intention

Research indicates that users who perceive the severe consequences of not adhering to recommended security policies are likelier to engage in protective behavior against phishing threats [36]. Similarly, an entrepreneur's perception of the severity of ransomware risk influences their likelihood to take preventive measures; the more severe the perceived risk, the higher the probability that an entrepreneur will engage in protective behaviors to safeguard their business against ransomware attacks [17]. Moreover, perceived severity has been found to have a substantial effect on the intention and behavior of users regarding security practices, with severity having the most substantial effect on protection behavior among all other factors considered [31]. Therefore, this led to the formulation of the following hypothesis:

H9: *Perceived severity positively affects security behavior intention in avoiding clicking on phishing emails.*

2.3.10 Perceived vulnerability and security behavior intention

Research suggests that perceived risk vulnerability significantly influences behavioral intention toward security behaviors. For instance, a study on smartphone security behavior found that perceived risk vulnerability more substantially impacts behavioral intention among female employees than male employees. This highlights how individuals assess their likelihood of security risks materializing, which subsequently shapes their intention to adopt protective behaviors [11]. Similarly, those who perceive themselves as more vulnerable to cyber fraud and cybercrime are more inclined to take protective measures. This aligns with the Protection Motivation Theory, which posits that higher perceived vulnerability motivates individuals to take proactive security actions [37]. Furthermore, enhancing users perceived vulnerability by educational and awareness programs can strengthen the intention to engage in security behaviors. Educating employees about phishing risks and the cybersecurity measures importance increase their perception of vulnerability, encouraging a substantial commitment to protective actions [38]. Therefore, this led to the formulation of the following hypothesis:

H10: *Perceived vulnerability is a positive predictor for security behavior intention in avoiding clicking on phishing emails.*

2.3.11 Self-efficacy and security behavior intention

Research indicates a positive relationship between self-efficacy and security behavior intention. Employees with greater confidence in their ability to perform security-related actions tend to reflect it through their protective behaviors [14]. Additionally, a higher level of self-efficacy can boost employees' behavioral intention to ensure the security of their smartphones, making the effect stronger among male employees [11]. Furthermore, self-efficacy positively impacts security behaviors, and increased situational support is proposed to enhance self-efficacy, which, in turn, may influence individuals to engage more effectively in information security measures [39]. Therefore, this led to the formulation of the following hypothesis:

H11: *Self-efficacy positively affects security behavior and the intention to avoid clicking on phishing emails.*

2.3.12 Response efficacy and security behavior intention

Research highlights a positive correlation between response efficacy and intention to engage in security behavior among entrepreneurs. Entrepreneurs who believe their actions effectively mitigate ransomware risks tend to engage more in protective behaviors to secure their business from cybercrimes [17]. Similarly, response efficacy positively impacts the comprehensiveness of cybersecurity behavior, as individuals who trust the effectiveness of their protective measures are likely to adopt intentional and thorough cybersecurity practices [39]. Furthermore, an individual's belief in the effectiveness of their responses to threats directly enhances their intention to engage in protective actions [40]. Therefore, this led to the formulation of the following hypothesis:

H12: *Response efficacy is a positive predictor for security behavior intention in avoiding clicking on phishing emails.*

3. METHODS

3.1 Research design

This study employed a quantitative, cross-sectional research design to examine the cybersecurity behavior among SOE employees. Data was analyzed using Structural Equation Modeling (SEM) with SmartPLS version 4.10 software. SmartPLS is particularly appropriate for exploratory studies because it can effectively handle complex models, non-normal data distributions, and small sample sizes [41, 42].

3.2 Sampling strategy and data collection

A purposive sampling strategy was adopted to ensure the sample was representative of the target population. The selection criteria focused on SOE employees, given the increasing frequency of phishing email attacks targeting this demographic in recent months. The data was collected through an online questionnaire distributed via Google Forms over two months, from March to April 2024. Eligibility criteria were implemented to ensure the quality and relevance of responses.

3.3 Sample size determination

The study employed G-Power analysis to determine the appropriate sample size [43]. A priori power analysis was conducted using F-tests for linear multiple regression, with parameters set at a power value of 0.95, an alpha level of 0.05, six predators, and an effect size of 0.15 [44, 45], although the analysis recommended sample size of 146, a larger sample of 189 was utilized to ensure a higher response rate and mitigate the risk of non-response bias.

3.4 Questionnaire development and measures

The questionnaire item of threat awareness and self-efficacy was adapted from study [17], security awareness was adapted from [14, 34]. Perceived severity, perceived vulnerability, response efficacy, and security behavior intention was adapted from the study [14]. The indicator was measured using a five-point Likert scale, with one is strongly disagree and five strongly agree. Following the translation and editing of the

questions from prior research, a fluent English speaker assessed the final version to detect any flaws.

3.5 Content validation

Two subject matter experts in management and information systems evaluated the questionnaire for content validity. The evaluation focused on overall format and structure, linguistic clarity and coherence, and eliminating ambiguous or redundant items. The received feedback was then used to improve the questionnaire's clarity and reliability.

3.6 Ethical consideration

The consent statement provided at the beginning of the questionnaire highlights the research purpose, the respondent's rights, the privacy and data security policy, the anticipated data usage, and the approval request. This ensured that additional safeguards were made to protect the respondents' information.

3.7 Pilot testing

A pilot test was conducted with 30 respondents from financial and non-financial SOEs to assess the quiestionnaire's reliability and validity [46]. The researchers examined the respondents who met the predetermined criteria to evaluate the initial internal coherence. Except for SA1 (0.476) and PS3 (0.520), all structures demonstrated good internal reliability results during the pilot testing. The composite reliability (CR) values ranged from 0.775 (SA) to 0.897 (SE), while the average variance extracted (AVE) values ranged from 0.549 (SA) to 0.719 (RE). The comprehensive data collection can commence following the approval of the AVE values for SA (0.549) and PS (0.662), despite two indicators failing to meet the standards for internal consistency reliability.

3.8 Data analysis procedure

The previous researchers suggested a conceptualization model incorporating a reflective strategy [47]. The previous researchers stated that the data was assessed utilizing convergent and discriminant validity, internal consistency, and factor reliability [48]. The previous researchers examined the structural model and its associated hypotheses after the completion of the confirmatory factor analysis phase and the fulfillment of all requisite requirements [48]. The efficacy of the proposed model in generating accurate predictions was assessed using the PLS predict method by previous study [49]. Identifying prior versions that had mediocre performance but were vital to the intended structures was performed by applying importance-performance map analysis (IPMA) [50]. The results and discussions section thoroughly and extensively explains the procedure.

4. RESULTS AND DISCUSSIONS

4.1 Descriptive and data normality analysis

In this study, the researchers obtained 189 respondents. The research started off by conducting a normal test by assessing excess kurtosis and skewness. Table 1 shows the normality test using kurtosis and skewness values. The data can be considered a normal distribution when the kurtosis and skewness are between -1 and + 1 [51]. The kurtosis and skewness values ranged from -0.891 (SE2) to 1.246 (PS2) and -1.411 (PS2) to -0.246 (SE2). Therefore, the researchers determine that the data is not normally distributed as several indicators fail to meet the criteria. However, several studies using SEM with SmartPLS did not require the data to be distributed normally [52]. The researcher subsequently conducts a descriptive analysis of the respondent profile. Table 1 shows the descriptive analysis of the respondent profile. The researchers concluded that the majority of the respondents are male (71.43%), between the age range of 26-45 years (88.89%), with the education background of bachelor's degree and high school (88.36%), and financial sector (60.85%).

Table 1. Descriptive analysis of respondent profile

Description		Frequency/Percentage
Gender	Male	135/71.43%
	Female	54/28.57%
Age Group	26-35 y.o	136/71.96%
	36-45 y.o	32/16.93%
	15-25 y.o	13/6.88%
	46-56 y.o	8/4.23%
Education Level	Bachelor Degree	144/76.19%
	High School	23/12.17%
	Master Degree	14/7.41%
	Diploma	8/4.23%
Industry	Financial Sector	115/60.85%
	Non-Financial Sector	74/39.15%

4.2 Measurement model evaluation

Next, the researchers perform confirmatory factor analysis (CFA) by examining the individual indicator consistency, internal consistency reliability, convergent validity, and discriminant validity. The researchers employ cut-off values that previous researchers widely used. The outer loading, composite reliability, and AVE a minimum of 0.6, 0.7, and 0.5, respectively [47]. CFA is a statistical technique to examine the validity of indicators and variables. The AVE measures the variance captured by a latent construct concerning the variance due to measurement error. Table 2 shows the convergent validity and internal consistency reliability. The outer loading value ranged from 0.661 (SE4) to 0.878 (PS2). The composite reliability value ranged from 0.788 (TA) to 0.868 (RE). The AVE value ranged from 0.526 (SE) to 0.687 (RE). Table 2 shows the convergent validity and internal consistency reliability test results. Therefore, the researchers concluded that the individual indicator consistency, internal consistency reliability, and convergent validity meet the criteria.

Next, the researchers conduct discriminant validity using the Fornell-Larcker criterion to confirm each construct is distinct from other constructs in the model. Table 3 shows the discriminant validity results. The Fornell-Larcker criterion was used due to reliability, simplicity, ease of interpretation, and relevance to the research context [41, 42]. The researchers conclude that the model meets the criterion. Therefore, the model shows satisfactory discriminant validity.

Table 2. Normality, individual indicator consistency, convergent validity, and internal consistency reliability

Variable and Indicator	1	2	3	4	5	6
Perceived Severity (PS):						
Companies can incur significant losses (in terms of finances, time, or privacy) when getting attacked by ransomware (PS1)	0.634	-1.091	4.159	0.794		
I will be penalized for violating the company's security policy (PS2)	1.246	-1.411	4.275	0.878	0.862	0.675
Having a computer infection due to opening suspicious email attachments is a serious problem for me (PS3)	0.500	-1.175	4.180	0.790		
Perceived Vulnerability (PV):						
If I do not comply with the company security policy, it may cause security issues with company information (PV1)	0.061	-0.926	4.196	0.819		
The company becomes vulnerable to a security breach if I do not comply with existing information security policies. (PV2)	-0.700	-0.632	4.111	0.793	0.855	0.663
If I do not comply with my agency's information security policy, then I could fall victim to a malicious attack (PV3)	0.037	-0.981	4.175	0.829		
Response Efficacy (RE):						
I believe I can evaluate the risk to my work entity if I get an email phishing attack (RE1)	0.383	-1.022	4.212	0.819		
I am sure I can protect my work entity from email phishing attacks (RE2)	-0.124	-0.885	4.169	0.821	0.868	0.687
I believe I can identify email phishing attacks (RE3)	-0.241	-0.792	4.233	0.846		
Security Awareness (SA):						
The company has an information security policy (SA1)	-0.100	-0.860	4.079	0.731		
The company reminded me to implement computer and Internet security policies (SA2)	-0.032	-0.871	4.026	0.776	0.813	0.593
I have a high awareness of the risks of clicking on suspicious email links (SA3)	0.654	-1.129	4.190	0.800		
Security Behavior Intention (SBI):						
I keep the antivirus software on my computer up to date (SBI1)	-0.246	-0.604	3.937	0.704		
I monitor unusual computer behavior (e.g., slow or freezing, pop-up windows, etc.) (SBI2)	-0.368	-0.677	3.974	0.777	0.798	0.569
I always act immediately when malware alerts appear (SBI3)	0.174	-0.854	4.169	0.779		
Self-Efficacy (SE):						
I believe I can evaluate the risk to my work entity if I get an email phishing attack (SE1)	-0.284	-0.497	3.794	0.767		
I am sure I can protect my work entity from email phishing attacks (SE2)	-0.891	-0.246	3.746	0.712	0.815	0.526
I believe I can identify email phishing attacks (SE3)	-0.382	-0.401	3.688	0.755		
I am confident I can take the necessary action if my work entity is hit by an email phishing attack (SE4)	-0.417	-0.398	3.704	0.661		
Threat Awareness (TA):						
I understand that a ransomware attack could hit my organization. (TA1)	-0.381	-0.441	3.847	0.683		
I understand that hackers can install ransomware on my working devices. (TA2)	-0.446	-0.738	4.048	0.768	0.788	0.554
I understand what happens when ransomware is installed on my working devices. (TA3)	-0.155	-0.672	4.085	0.777		

1 = Kurtosis, 2 = Skewness, 3 = Mean, 4 = Outer loading, 5 = Composite reliability, 6 = AVE.

Table 3. Discriminant validity Fornell-Larcker criterion

	1	2	3	4	5	6	7
1	0.822						
2	0.657	0.814					
3	0.637	0.795	0.829				
4	0.719	0.692	0.679	0.770			
5	0.519	0.599	0.555	0.513	0.754		
6	0.226	0.325	0.320	0.326	0.485	0.725	
7	0.507	0.630	0.654	0.595	0.601	0.444	0.744

Note: 1: Perceived Severity; 2: Perceived Vulnerability; 3: Response Efficacy; 4: Security Awareness; 5: Security Behavior Intention; 6: Self-efficacy; 7: Threat Awareness.

4.3 Structural model evaluation

Next, the researchers perform the structural model examination, the coefficient of determination, and the predictive power. The researchers select a one-tailed test, a sub-sample size of 5,000, and a bias-corrected and accelerated (Bca) bootstrap. The Bias-corrected and accelerated (Bca) confidence interval method for 0.025 was applied. The f^2 statistic was used to illustrate the influence of independent variables on the dependent variables. Different levels of effect are presented as follows: high ($f^2 > 0.350$), moderate ($f^2 > 0.150$), and minor ($f^2 > 0.020$) [53]. Furthermore, a composite criterion consisting of p-values and effect sizes can give a better understanding of the data [54, 55]. In Table 3, the outcome of hypothesis testing shows that all hypotheses were accepted.

The results of the structural model depicted that self-efficacy (H_{11}, $\beta = 0.315$), perceived vulnerability (H_{10} accepted, $\beta = 0.288$), and perceived severity (H_9 accepted, $\beta = 0.193$) positively affect security behavior intention. However, response efficacy found not significant (H_{12} rejected, $\beta = 0.103$). Therefore, the researchers conclude that perceived severity is critical for determining security behavior intention.

Next, threat awareness positively affects response efficacy (H_4 accepted, $\beta = 0.387$), perceived vurnerability (H_2 accepted, $\beta = 0.339$), and self-efficacy (H_3 accepted, $\beta = 0.387$). However, the relationship between thread awareness and perceived severity was insignificant (H_1 rejected, $\beta = 0.122$). Therefore, the researchers conclude that threat awareness moderately affects response efficacy and perceived vulnerability.

Finally, security awareness positively affects perceived severity (H_5 accepted, $\beta = 0.646$), perceived vulnerability (H_6

accepted, β = 0.490), and response efficacy (H_8 accepted, β = 0.449). However, the relationship between security awareness and self-efficacy found not significant (H_7 rejected, β = 0.096). Therefore, the researchers conclude that security awareness highly affects perceived severity (Table 4).

Table 4. Hypothesis test result

Hypothesis	β	Stdev	T-Stat	P-Values	BCI LL	BCI UL	F^2
H1: TA ->PS	0.122	0.088	1.395	0.082	-0.050	0.285	0.020
H2: TA -> PV	0.339	0.072	4.726	0.000	0.196	0.475	0.166
H3: TA -> SE	0.387	0.089	4.354	0.000	0.193	0.543	0.122
H4: TA -> RE	0.387	0.069	5.609	0.000	0.251	0.522	0.218
H5: SA -> PS	0.646	0.064	10.166	0.000	0.518	0.763	0.570
H6: SA -> PV	0.490	0.068	7.241	0.000	0.358	0.624	0.347
H7: SA -> SE	0.096	0.091	1.058	0.145	-0.074	0.279	0.007
H8: SA -> RE	0.449	0.076	5.929	0.000	0.297	0.592	0.294
H9: PS -> SBI	0.193	0.084	2.284	0.011	0.049	0.379	0.038
H10: PV ->SBI	0.288	0.098	2.951	0.002	0.103	0.484	0.052
H11: SE -> SBI	0.315	0.071	4.421	0.000	0.173	0.453	0.170
H12: RE -> SBI	0.103	0.096	1.074	0.141	-0.082	0.300	0.007

Note: R^2 of SBI = 40.3%; PS = 32.4%; PV = 38.9%; RE = 32.2%; SE = 39.5%; PS: Perceived Severity; PV: Perceived Vulnerability; RE: Response Efficacy; SA: Security Awareness; Security Behavior Intention; SE: Self-efficacy; TA: Threat Awareness.

4.4 PLS predict evaluation

Next, the researchers perform the PLS prediction analysis to evaluate the predictive capability to assess how well the model predicts data, focusing on the relevance of the endogenous construct [49]. The researchers employ 10 10-fold cross-validation methods with 10 repetitions. The researchers select the Means Absolute Error (MAE) because the data is not normally distributed. The researchers evaluate the PLS_MAE to have naïve lower linear regression (LM) MAE. Table 5 shows the predictive efficacy of PLS predict. It is concluded that the model shows a low predictive power due to a minority of the dependent indicators producing lower PLS_MAE than LM_MAE.

Table 5. PLS predict

Indicators	1	2	3	4
SBI1	0.138	0.862	0.687	-0.021
SBI2	0.182	0.886	0.726	-0.016
SBI3	0.293	0.745	0.601	-0.011

Note: 1: Q^2predict; 2: PLS-SEM_MAE; 3: LM_MAE; 4: Δ PLS-SEM_MAE - LM_MAE.

4.5 Importance-performance map analysis

Finally, the researchers performed a significant performance map analysis to enhance the PLS-SEM results and the important improvement factors [50]. Figure 1 shows the IPMA of security behavior intention. The researchers classify security awareness, self-efficacy, perceived vulnerability, and threat awareness in quadrant II (concentrate here). Moreover, the perceived severity is in quadrant IV (possible overkill), and response efficacy falls in quadrant III (low priority).

Based on IPMA of security behavior, the researchers identify managerial implications: Management can increase security awareness through training activities on protecting company data and strategies to protect employees through increasing awareness about cyber security. In addition, it is important to use passwords that are not easy to hack and change every 6 months. Improving the security system through implementing multi-factor authentication needs to be considered for implementation to improve the security of important company data.

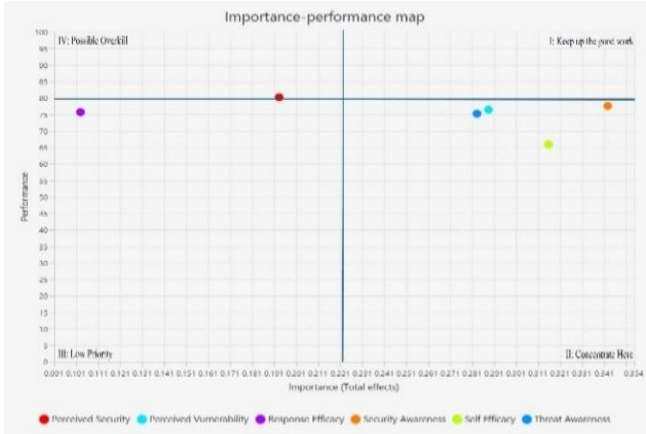

Figure 1. Importance performance map analysis of security behavior intention

At the individual employee level, management needs to pay attention to improving each employee's self-efficacy. Management needs to cultivate knowledge sharing about how hackers' modus operandi, the impact on hacking victims, and the level of vulnerability of individuals to hacker attacks. This can provide reasonable confidence for users to be careful when using the internet. In addition, ongoing training development programs and campaigns on how employees' computers are infected with computer viruses can also increase employee confidence in daily activities.

Management needs to introduce how every employee is vulnerable to cyber-attacks. The development of training modules that focus on introducing phishing, trojans, password keyloggers, and how a hacker's modus operandi of obtaining bank account authorizations can equip employees with knowledge of the risks of cyber-attacks. Therefore, training activities like this are very beneficial for employees to avoid access to suspicious emails, text messages, and website links.

Another thing that can be developed to increase employee threat awareness against cyber-attacks is the development of educational programs based on infographics, simulations, video tutorials, and interactive games delivered through the company's learning management system. In the end, how to manage policies to force employees at the operational, middle, and top management levels to access, follow, and implement the results of educational programs that have been developed

thoughtfully.

Finally, it is crucial for the management to develop and implement a detection and curation approach when the preventive measures fail. Management needs must allocate resources in security tools analysis such as data and system backup, incident response, and threat detection, and periodically perform risk analysis.

4.6 Discussions

Self-efficacy was reported to affect security behavior intention moderately (H_{11} accepted). This finding aligns with the previous research [11, 14, 39]. Next, perceived vulnerability does not affect security behavior intention (H_{10} accepted). This finding is consistent with the previous research [11, 36, 38]. Next, perceived severity does not affect security behavior intention (H_9 accepted). This finding is consistent with the previous research [17, 34]. Finally, response efficacy was to be not significant in terms of security behavior intention (H_{12} rejected). This finding argues the previous research finding [17, 39, 40].

It was reported that threat awareness moderately affects response efficacy (H_4 accepted). This finding is consistent with the previous research [17, 30-32]. Next, threat awareness moderately affects perceived vulnerability (H_2 accepted). This finding is consistent with the previous research [13, 27, 28]. Next, threat awareness shows a negligible effect on self (H_3 accepted). This finding is consistent with the previous research efficacy [17, 28-30]. Finally, threat awareness was insignificant in perceived severity (H_1 rejected). This finding argues the previous research finding [10, 13, 24, 25].

Security awareness was reported to highly affect perceived severity (H_5 accepted). This finding is consistent with the previous research [10, 14, 18]. Next, security awareness moderately affects perceived vulnerability (H_6 accepted). This finding is consistent with the previous research [10, 14, 55]. Next, security awareness moderately affects response efficacy (H_8 accepted). This finding is consistent with the previous research [10, 13, 15, 18]. Finally, security awareness was not significant in self-efficacy (H_7 rejected). This finding argues the previous research finding [15, 34, 35].

5. CONCLUSIONS

Our research examines the determinant factors of security behavior intention in state-owned organizations. The researchers extend the protection motivation theory with security and threat awareness. The findings show that self-efficacy, perceived vulnerability, and perceived severity are important factors of security behavior intention. Moreover, threat awareness can be important in response efficacy, perceived vulnerability, and self-efficacy. Finally, security awareness can be considered an important factor in perceived severity, vulnerability, and response efficacy.

However, three hypotheses are rejected (threat awareness on perceived severity, security awareness on self-efficacy, and response efficacy on security behavior intention). Contradictory results in hypothesis tests can be caused by educational background, age group, and occupation in the financial sector. In their daily work, the respondents face the threat of online crime, so a character is formed who is always alert to the threat of online crime and follows the development of cybersecurity.

The proposed model shows good coefficient determination despite low predictive power. The researchers used IPMA to strengthen managerial implications. The findings significantly contribute to the state-owned organization management strengthening employee awareness of cyber threats, especially email phishing. The proposed risk management strategies have been discussed in the previous section. The researchers feel that preventive, detective, and curative activities must be considered and executed by the IT and human resources management division.

Our research contributes to advancing cyber security behavior research, especially the role of protection motivation theory application. The proposed model shows the importance of incorporating security and threat awareness as determinant factors of perceived vulnerability, self-efficacy, perceived severity, and response efficacy of email phishing threats. Next, our proposed model can be applied in cyber security behavior research, especially in state-owned organizations. Finally, we employ rigorous methodology to ensure and enrich the existing research findings.

Finally, our research has several limitations in its design and execution. Therefore, we propose some future research directions for further researchers. First, applying g-power analysis to determine sample size is trending nowadays. However, the purposive sampling selected as the sampling strategy has limitations for the generalization of findings. Future researchers need to increase the sample size and employ probability sampling to generalize findings potentially. Second, the researchers gathered 60.85% of the total respondents (115 of 189) from the financial sector. Therefore, the findings mainly apply to the financial sector due to the highly regulated industry. The researchers suggest replicating the proposed model to specific state-owned organizations like banking, insurance, agriculture, electricity, or telecommunication. Lastly, the researchers have examined the effect of security and threat awareness in existing studies. Those variables explained 32.4%-39.5% of perceived vulnerability, response efficacy, self-efficacy, and perceived severity. Future research might consider the effect of cultural, cyber security literacy, and personality trait factors on protection motivation theory.

AUTHOR CONTRIBUTIONS

The following statements were used: Conceptualization, A.M.S, and O.A.; methodology, A.M.S, O.A., R.A.A., and B.L.; software, A.M.S and O.A.; validation, A.M.S, O.A., R.A.A., and B.L.; formal analysis, A. M. S., R.A.A., and B.L.; investigation, A.M.S. and O.A; resources, A.M.S, O.A., R.A.A., and B.L.; data curation, A.M.S and O.A.; writing—original draft preparation, O.A., R.A.A., and B.L; writing—review and editing, A.M.S.; visualization—A.M.S; supervision—A.M.S.; project administration—A.M.S,; funding acquisition, N/A. All authors have read and agreed to the published version of the manuscript.

DATA AVAILABILITY STATEMENT

The data supporting this study's findings are not publicly available due to privacy and confidentiality concerns. Access to the data may be granted upon reasonable request and after appropriate approval, ensuring compliance with data

protection regulations. Please contact the corresponding author for further information regarding data access. The data can be downloaded through bit.ly/40bv0m9.

REFERENCES

[1] Adane, K., Beyene, B. (2023). Email and website-based phishing attack: Examining online users security behavior in cyberspace environment. International Journal of Information Science and Management, 21(1): 245-262. https://doi.org/10.22034/IJISM.2022.1977800.0

[2] Alneyadi, M.R.M.A.H., Normalini, M.K. (2023). Factors influencing user's intention to adopt AI-based cybersecurity systems in the UAE. Interdisciplinary Journal of Information, Knowledge, and Management, 18: 459-486. https://doi.org/10.28945/5166

[3] Al-Balushi, A., Tarhini, A., Acikgoz, F., Ali, S. (2023). Examining the factors that influence user information security behavior toward COVID-19 scams. International Journal of Human-Computer Interaction, 40(24): 8809-8826 https://doi.org/10.1080/10447318.2023.2291608

[4] Aldawood, H., Skinner, G. (2020). An advanced taxonomy for social engineering attacks. International Journal of Computer Applications, 177(30): 1-11. https://doi.org/10.5120/IJCA2020919744

[5] Alfalah, A.A. (2023). The role of internet security awareness as a moderating variable on cyber security perception: Learning management system as a case study. International Journal of Advanced and Applied Sciences, 10(4): 136-144. https://doi.org/10.21833/ijaas.2023.04.017

[6] Alrfai, M.M., Alqudah, H., Lutfi, A., Al-Kofahi, M., Alrawad, M., Almaiah, M.A. (2023). The influence of artificial intelligence on the AISs efficiency: Moderating effect of the cyber security. Cogent Social Sciences, 9(2): 2243719. https://doi.org/10.1080/23311886.2023.2243719

[7] Al-Somali, S.A., Saqr, R.R., Asiri, A.M., Al-Somali, N.A. (2024). Organizational cybersecurity systems and sustainable business performance of small and medium enterprises (SMEs) in Saudi Arabia: The mediating and moderating role of cybersecurity resilience and organizational culture. Sustainability, 16(5): 1880. https://doi.org/10.3390/SU16051880

[8] Ameen, N., Tarhini, A., Hussain Shah, M.H., Madichie, N.O. (2020). Employees' behavioral intention to smartphone security: A gender-based, cross-national study. Computers in Human Behavior, 104: 106184. https://doi.org/10.1016/j.chb.2019.106184

[9] Badan Siber dan Sandi Negara. (2023). BSSN Ungkap Lanskap Keamanan Siber Indonesia Tahun 2022 untuk Literasi Budaya Keamanan Siber. https://www.bssn.go.id/lanskap2022/.

[10] Berens, B.M., Schaub, F., Mossano, M., Volkamer, M. (2024). Better together: The interplay between a phishing awareness video and a link-centric phishing support tool. In Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems, Honolulu, USA, pp. 826. https://doi.org/10.1145/3613904.3642843

[11] Bokhari, S.A.A., Myeong, S. (2023). The influence of artificial intelligence on e-governance and cybersecurity in smart cities: A stakeholder's perspective. IEEE Access, 11: 69783-69797. https://doi.org/10.1109/ACCESS.2023.3293480

[12] Brown, S., Ruhwanya, Z., Pekane, A. (2023). Factors influencing internet of medical things (IoMT) cybersecurity protective behaviors among healthcare workers. In International Symposium on Human Aspects of Information Security and Assurance, Kent, United Kingdom, pp. 432-444. https://doi.org/10.1007/978-3-031-38530-8_34

[13] Candiwan, C., Azmi, M., Alamsyah, A. (2022). Analysis of behavioral and information security awareness among users of zoom application in COVID-19 era. International Journal of Safety and Security Engineering, 12(2): 229-237. https://doi.org/10.18280/ijsse.120212

[14] Cohen, J. (1988). Statistical Power Analysis for the Behavioral Sciences (2nd ed.). L. Erlbaum Associates.

[15] De Kimpe, L., Walrave, M., Verdegem, P., Ponnet, K. (2022). What we think we know about cybersecurity: An investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. Behavior and Information Technology, 41(8): 1796-1808. https://doi.org/10.1080/0144929X.2021.1905066

[16] Dodge, C.E., Fisk, N., Burruss, G.W., Moule, R.K., Jaynes, C.M. (2023). What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. Criminology and Public Policy, 22(4): 849-868. https://doi.org/10.1111/1745-9133.12641

[17] Dubyna, M., Verbivska, L., Kalchenko, O., Dmytrovska, V., Pilevych, D., Lysohor, I. (2023). The role of digitalization in ensuring the financial and economic security of trading enterprises under the conditions of external shocks. International Journal of Safety and Security Engineering, 13(5): 821-833. https://doi.org/10.18280/IJSSE.130506

[18] Fei, Z., Normalini, M.K., Mohamad, W.N. (2023). Investigating factors affecting the intention to use mobile health from a holistic perspective: The case of small cities in China. Interdisciplinary Journal of Information, Knowledge, and Management, 18: 739-767. https://doi.org/10.28945/5196

[19] Ghazali, N. N., Hassan, S., Ahmad, R. (2023). Fortifying against cyber fraud: Instrument development with the protection motivation theory. International Journal of Advanced Computer Science and Applications, 14(10): 519-526. https://doi.org/10.14569/IJACSA.2023.0141055

[20] Hassan, S., Ahmad, R., Katuk, N., Ghazali, N.N., Aripin, J.A., Ali, F. (2024). Staying one step ahead: Exploring protection motivation theory to combat cyber-fraud among e-services users. Procedia Computer Science, 234: 1364-1371. https://doi.org/10.1016/j.procs.2024.04.011

[21] Gu, T. (2025). Restrictions on Chinese SOE investments for data security reasons: The case of Australia. Chinese Journal of Transnational Law, 2(1): 14-38. https://doi.org/10.1177/2753412X241270432

[22] Hair, J., Alamer, A. (2022). Partial least squares structural equation modeling (PLS-SEM) in second language and education research: Guidelines using an applied example. Research Methods in Applied Linguistics, 1(3): 100027. https://doi.org/10.1016/J.RMAL.2022.100027

[23] Hair Jr, J.F., Hult, G.T.M., Ringle, C.M., Sarstedt, M., Danks, N.P., Ray, S. (2021). Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R: A Workbook. Springer Nature.
[24] Hamzah, M.I. (2024). Fear of COVID-19 disease and QR-based mobile payment adoption: A protection motivation perspective. Journal of Financial Services Marketing, 29(3): 946-963. https://doi.org/10.1057/s41264-023-00246-4
[25] Hanus, B., Wu, Y.A. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. Information Systems Management, 33(1): 2-16. https://doi.org/10.1080/10580530.2015.1117842
[26] Hassandoust, F., Techatassanasoontorn, A.A. (2019). Understanding users' information security awareness and intentions: A full nomology of protection motivation theory. In Cyber Influence and Cognitive Threats, pp. 129-143. https://doi.org/10.1016/B978-0-12-819204-7.00007-5
[27] Haws, K.L., Sample, K.L., Hulland, J. (2023). Scale use and abuse: Towards best practices in the deployment of scales. Journal of Consumer Psychology, 33(1): 226-243. https://doi.org/10.1002/jcpy.1320
[28] Holmes, M., Ophoff, J. (2019). Online security behaviour: Factors influencing intention to adopt two-factor authentication. In 14th International Conference on Cyber Warfare and Security, Stellenbosch, South Africa, pp. 123-132.
[29] Hong, Y., Furnell, S. (2021). Understanding cybersecurity behavioral habits: Insights from situational support. Journal of Information Security and Applications, 57: 102710. https://doi.org/10.1016/J.JISA.2020.102710
[30] IDX Channel. (2022). 10 BUMN dengan Laba Terbesar: Siapa Setelah Telkom? https://www.idxchannel.com/economics/10-bumn-dengan-laba-terbesar-siapa-setelah-telkom.
[31] Badan Pusat Statistik. (2025). Penduduk Berumur 15 tahun ke atas menurut jenis kegiatan, 2024. https://www.bps.go.id/id/statistics-table/2/NTI5IzI=/penduduk-berumur-15-tahun-ke-atas-menurut-jenis-kegiatan.html.
[32] Ismail, K.A., Singh, M.M., Mustaffa, N., Keikhosrokiani, P., Zulkefli, Z. (2017). Security strategies for hindering watering hole cyber crime attack. Procedia Computer Science, 124: 656-663. https://doi.org/10.1016/j.procs.2017.12.202
[33] Jain, A.K., Debnath, N., Jain, A.K. (2022). APuML: An efficient approach to detect mobile phishing webpages using machine learning. Wireless Personal Communications, 125(4): 3227-3248. https://doi.org/10.1007/s11277-022-09707-w
[34] Le, L.H., Hoang, A.P., Pham, H.C. (2023). Factors affecting prosocial sharing health-related information on social media during a health crisis: A dual exchanging-protecting model. Australasian Journal of Information Systems, 27: 1-25. https://doi.org/10.3127/AJIS.V27I0.4349
[35] Le, T.D., Le-Dinh, T., Uwizeyemungu, S. (2024). Search engine optimization poisoning: A cybersecurity threat analysis and mitigation strategies for small and medium-sized enterprises. Technology in Society, 76: 102470. https://doi.org/10.1016/J.TECHSOC.2024.102470
[36] Li, L., Xu, L., He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. Computers in Human Behavior Reports, 5: 100165. https://doi.org/10.1016/j.chbr.2021.100165
[37] Li, Y., Yang, R., Lu, Y. (2024). A privacy risk identification framework of open government data: A mixed-method study in China. Government Information Quarterly, 41(1): 101916. https://doi.org/10.1016/J.GIQ.2024.101916
[38] Bekkers, L., van't Hoff-De Goede, S., Misana-ter Huurne, E., van Houten, Y., Spithoven, R., Leukfeldt, E.R. (2023). Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model. Computers & Security, 127: 103099. https://doi.org/10.1016/j.cose.2023.103099
[39] Martens, M., De Wolf, R., 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, 92: 139-150. https://doi.org/10.1016/j.chb.2018.11.002
[40] Mayr, S., Erdfelder, E., Buchner, A., Faul, F. (2007). A short tutorial of GPower. Tutorials in Quantitative Methods for Psychology, 3(2): 51-59.
[41] Mishra, P., Pandey, C.M., Singh, U., Gupta, A., Sahu, C., Keshri, A. (2019). Descriptive statistics and normality tests for statistical data. Annals of Cardiac Anaesthesia, 22(1): 67-72. https://doi.org/10.4103/ACA.ACA_157_18
[42] Mou, J., Cohen, J., Bhattacherjee, A., Kim, J. (2022). A test of protection motivation theory in the information security literature: A meta-analytic structural equation modeling approach. Journal of the Association for Information Systems, 23(1): 196-236. https://doi.org/10.17705/1jais.00723
[43] Pham, Q.T., Tran, X.P., Misra, S., Maskeliunas, R., Damaševičius, R. (2018). Relationship between convenience, perceived value, and repurchase intention in online shopping in Vietnam. Sustainability, 10(1): 156. https://doi.org/10.3390/su10010156
[44] Pham, T.H., Phan, T.A., Trinh, P.A., Mai, X.B., Le, Q.C. (2024). Information security risks and sharing behavior on OSN: The impact of data collection awareness. Journal of Information, Communication and Ethics in Society, 22(1): 82-102. https://doi.org/10.1108/JICES-06-2023-0076
[45] Purwanti, T. (2022). 5 Perusahaan BUMN dengan Gaji Tertinggi, Capai Ratusan Juta? https://www.cnbcindonesia.com/market/20220623090607-17-349541/5-perusahaan-bumn-dengan-gaji-tertinggi-capai-ratusan-juta.
[46] Rahimpour, H., Tusek, J., Musleh, A.S., Liu, B., Abuadbba, A., Phung, T., Seneviratne, A. (2024). A review of cybersecurity challenges in smart power transformers. IEEE Access, 12: 193972-193996. https://doi.org/10.1109/ACCESS.2024.3518494
[47] Rawindaran, N., Jayal, A., Prakash, E., Hewage, C. (2023). Perspective of small and medium enterprise (SME's) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales. International Journal of Information Management Data Insights, 3(2): 100191.

https://doi.org/10.1016/J.JJIMEI.2023.100191
[48] Ringle, C.M., Sarstedt, M. (2016). Gain more insight from your PLS-SEM results: The importance-performance map analysis. Industrial Management & Data Systems, 116(9): 1865-1886. https://doi.org/10.1108/IMDS-10-2015-0449
[49] Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change1. The Journal of Psychology, 91(1): 93-114. https://doi.org/10.1080/00223980.1975.9915803
[50] Sarstedt, M., Hair Jr, J.F., Ringle, C.M. (2023). "PLS-SEM: Indeed a silver bullet"–Retrospective observations and recent advances. Journal of Marketing theory and Practice, 31(3): 261-275. https://doi.org/10.1080/10696679.2022.2056488
[51] Shmueli, G., Sarstedt, M., Hair, J.F., Cheah, J.H., Ting, H., Vaithilingam, S., Ringle, C.M. (2019). Predictive model assessment in PLS-SEM: Guidelines for using PLS predict. European Journal of Marketing, 53(11): 2322-2347. https://doi.org/10.1108/EJM-02-2019-0189
[52] Sulaiman, N.S., Fauzi, M.A., Hussain, S., Wider, W. (2022). Cybersecurity behavior among government employees: The role of protection motivation theory and responsibility in mitigating cyberattacks. Information, 13(9): 413. https://doi.org/10.3390/info13090413
[53] Vrhovec, S., Mihelič, A. (2021). Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation. Computers & Security, 106: 102309. https://doi.org/10.1016/J.COSE.2021.102309
[54] Wang, X., Li, Y., Khasraghi, H.J., Trumbach, C. (2023). The mediating role of security anxiety in internet threat avoidance behavior. Computers and Security, 134: 103429. https://doi.org/10.1016/j.cose.2023.103429
[55] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., Basim, H.N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, 62(1): 82-97. https://doi.org/10.1080/08874417.2020.1712269