International Journal of Safety and Security Engineering
Vol. 15, No. 6, June, 2025, pp. 1229-1241
Journal homepage: http://iieta.org/journals/ijsse

Cybersecurity Compliance and Other Factors Influencing Employee Protective Behavior: A Case Study of Bank X in Indonesia

Andi Amelia Putri Maharani Akib, Candiwan Candiwan*, Dian Puteri Ramadhani

School of Economics and Business, Telkom University, Bandung 40287, Indonesia

Corresponding Author Email: candiwan@telkomuniversity.ac.id

https://doi.org/10.18280/ijsse.150613

Received: 26 March 2025
Revised: 15 May 2025
Accepted: 15 June 2025
Available online: 30 June 2025

Keywords:
employee protective behavior, information security policy compliance, SETA programs, financial institutions

ABSTRACT

Indonesia's banking sector faces over 1 million daily cyberattacks, with human error causing 80% of security breaches, yet existing cybersecurity research predominantly focuses on technology solutions rather than employee behavior within high-regulation environments. This study addresses a critical research gap by investigating how organizational levers—policy provision and Security Education, Training, and Awareness (SETA) programs—influence employee cybersecurity compliance behavior in Indonesia's banking industry. We surveyed 360 employees from Bank X (a consortium of Indonesia's three largest state-owned banks) using PLS-SEM analysis. Our theoretical framework integrates Protection Motivation Theory and Theory of Planned Behavior to examine pathways from organizational interventions through cybersecurity awareness, compliance attitude, and ISPC intention to protective behavior. Nine of ten hypotheses were supported: policy provision and SETA programs significantly enhance cybersecurity awareness, cascading through compliance attitude and ISPC intention to drive protective behavior. Notably, protection motivation does not directly influence behavior, revealing a boundary condition for PMT in hierarchical contexts. This study delivers the first large-scale evidence from Indonesia's banking industry, demonstrating that clear policies and sustained SETA investment can turn human vulnerabilities into organizational resilience. Financial institutions should prioritize clear policies and comprehensive SETA programs as primary cybersecurity culture drivers.

1. INTRODUCTION

Digitalization improves the performance of banks, but it also increases operational risks, particularly information security threats [1]. The financial sector is currently confronted with one of its most significant risks: information security threats [2]. A comprehensive comprehension of the most frequently encountered cyber threats, including malware, phishing, and ransomware, is required in light of the ongoing concerns regarding cyberattacks in the banking sector [3]. Employees are responsible for the maintenance of a comprehensive information security system in the context of the accelerating digital transformation [4].

The organization's susceptibility to intrusions is frequently exacerbated by employees' failure to adhere to information security compliance protocols [5, 6]. According to a 2021 survey conducted by TalentLMS of 1,200 employees, 61% of those who had completed CSA training were unable to respond to the survey questions. Consequently, it is feasible that employees do not prioritize information security concerns [7]. Digitalization has rapidly reshaped Indonesia’s financial landscape, pushing banks to embrace mobile platforms, digital wallets, and real-time transaction systems. As of 2023, Bank Indonesia reported that digital banking transactions reached IDR 53,000 trillion, a significant increase from previous years. However, this growth comes with heightened cybersecurity risks. According to the National Cyber and Crypto Agency (BSSN), Indonesian financial institutions experience over 1 million attempted cyberattacks daily, with human error identified as the cause of approximately 80% of breaches. In response, the Indonesian Financial Services Authority (OJK) issued Regulation No. 38/POJK.03/2016, requiring banks to implement information security governance frameworks. Despite regulatory progress, employee compliance remains a critical weak point. Existing research often overlooks internal actors, especially staff, who are essential to safeguarding digital infrastructure. This study responds to that gap by focusing on Bank X, an Indonesia’s top three state-owned banks. By investigating how institutional factors such as policy provision and Security Education, Training, and Awareness (SETA) programs influence cybersecurity awareness and protective behavior, this study offers a contextualized model tailored to Indonesia’s high-risk, regulation-driven environment. A representative from one of Indonesia's largest banks disclosed that the institution is subjected to at least one million attempted cyberattacks on a daily basis. Human factors are responsible for approximately 80% of these attacks, which is alarming. The challenge of ensuring employee compliance with information security policies persists, and it is influenced by a variety of factors, including organizational policies, employee training, and other information security programs. We emphasize that the establishment of a culture of information security compliance is significantly influenced by the implementation of explicit policies and awareness initiatives, such as Security Education, Training, and Awareness (SETA) programs [8, 9]. These initiatives improve employees' understanding of secure behaviors and their accountability for protecting information systems. Additionally, employees' information security behaviors have been identified as being significantly influenced by psychological factors, including self-efficacy, response efficacy, and perceived barriers [10].

Previous research has concentrated on the security aspects of customer information, while the role of employees as administrators and parties responsible for company assets and customer data is frequently disregarded [11-13]. There is a lack of comprehensive research that addresses employee behavior in response to these challenges, which is particularly evident in Indonesia, where institutions are confronted with an increasing number of information security threats [14]. The initial line of defense that individuals, including bank employees, can undertake is to increase awareness of cybersecurity threats and promote safe practices [15].

Considering that the human factor is one of the primary causes of cyber-attacks in an organization, the issue of information security among bank employees is on the rise, as evidenced by the aforementioned phenomena and issues. The objective of this investigation is to evaluate the impact of employee cybersecurity awareness and behavior on protective attitudes toward information security at Bank X in Indonesia. Furthermore, this investigation investigates the impact of Bank X's governance on the cybersecurity awareness of its employees. The information presented in this study is anticipated to serve as a reference for Bank X and other financial institutions in order to enhance employee awareness and protective attitudes. This will enable companies to mitigate the risk of data breaches or incidents that could potentially harm the company. A study titled "Cybersecurity Compliance and Other Factors Influencing Employee Protective Behavior: A Case Study of Bank X in Indonesia".

2. LITERATURE REVIEW OF RELATED WORK

Specifically in the context of organizations, a study has dug deep into the variables impacting cybersecurity behavior [16]. The dynamics of information security have been the subject of numerous theories, but there is still no silver bullet when it comes to boosting awareness, encouraging protective behaviors, and guaranteeing compliance. One goal of conducting a literature review is to get to the heart of the cybersecurity practices' underlying theories, concepts, and relationships. This study is based on two theories: Protection Motivation Theory (PMT), and the Theory of Planned Behavior (TPB). To comprehend the ways in which intentions, attitudes, and perceived dangers influence cybersecurity behaviors, these models are crucial.

2.1 Theory of Planned Behavior (TPB)

Employees' attitudes, intentions, and subjective norms influence their behavior when it comes to information security, and Ajzen's TPB theory [17] offers a useful conceptual framework for analyzing this phenomenon. According to TPB, a positive outlook on information security can motivate workers to follow company policy on the subject, which in turn increases the likelihood that they will take precautions.

2.2 Protection Motivation Theory (PMT)

Cybersecurity awareness (how well people understand the significance of security practices), compliance attitude (how willing people are to follow security policies), and protective behavior (what people do to lessen the impact of cybersecurity threats) are the main factors in this study. The process by which people evaluate dangers and select suitable countermeasures is described by Rogers's [18] Protection Motivation Theory (PMT). According to PMT, the two primary factors that impact a person's choice to take preventive action are threat assessment and countermeasure evaluation.

2.3 Cybersecurity awareness

Cybersecurity awareness defined by Shaw et al. [19], denotes an individual's comprehension of the significance of data protection and their duty to safeguard company records. Employees' capacity to assess and handle information security issues is impacted by this level of awareness. According to Witte [20], people take into account their self-efficacy, perceived barriers, and response efficacy while evaluating possible responses to injury. Improving the culture of compliance and protective behaviors requires an awareness of these factors [21].

2.4 Cybersecurity behavior

The term "information security behaviors" describes the steps that people take to lessen the impact of any cyber dangers. highlights the significance of this conduct in identifying the dangers caused by improper acts [22]. Employees' levels of cybersecurity knowledge, attitudes, and intentions towards ISPC, as well as policy compliance, substantially impact their protective activities. When businesses gain a better grasp of these actions, they are better able to devise plans to boost information security and compliance [23].

2.5 Provision of policies

When it comes to following the organization's security measures, the security policy serves as the foundation that employees follow. According to Chan et al. [24], in order to make sure that everyone in the company knows what they should be doing to keep sensitive company data safe, there needs to be well-communicated policy. In addition, as pointed out by Hwang et al. [25], having well-defined policies helps raise awareness among employees and makes it apparent what happens if they don't follow the rules, which makes them more likely to comply with cybersecurity protocols. There is evidence that raising knowledge and encouraging compliance with security measures in the workplace can be achieved through the provision of appropriate policies. The primary research hypothesis is based on the preceding description and is: "H1: The provision of policies is positively associated with cybersecurity awareness".

2.6 SETA programs

An organization's cybersecurity culture can't be fully developed without the SETA (Security Education, Training, and Awareness) program. Employees will be better able to understand and comply with cybersecurity policies after completing this course. According to Alec Cram et al. [26], the SETA program raises staff members' knowledge of and capacity to handle security concerns using a variety of mediums, including training and seminars. Supporting policy awareness, shaping compliance attitudes, and encouraging employee protective conduct are all goals of an effective SETA program [16]. Emphasize that Cyber Threat Intelligence (CTI) awareness programs are crucial in Indonesian banks for mitigating cyberattacks and ensuring employee vigilance. Their findings support the role of structured SETA programs in strengthening cybersecurity behavior among bank employees in Indonesia [27]. To determine the best training formats for increasing cybersecurity awareness and to assess the particular efficacy of SETA programs in various organizational settings, additional empirical research is necessary. Hence, the study's second hypothesis is: "H2: SETA programs are positively related to cybersecurity awareness".

2.7 Intention toward ISPC

A key component in employee conduct is the degree to which they intend to adhere to ISPC (Information Security Policy Compliance). According to research by Wiafe et al. [28], when employees have a good outlook on ISPC, they are more likely to follow current security regulations. When workers are committed to following company policy, they are more likely to be consistent in their efforts to safeguard sensitive data and assets [16]. So, to conclude this analysis, the third hypothesis is: "H3: Cybersecurity awareness is positively associated with an intention towards ISPC".

2.8 Cybersecurity compliance attitude

The way someone feels has a significant impact on their reaction to potential security risks and their choice of action. An individual's perspective on cybersecurity matters in encouraging the right actions to lessen risk, as highlighted by Tran et al. [29]. When employees have a positive outlook on cybersecurity regulations, they are more likely to comprehend the significance of protecting information, which impacts their protective actions [30]. Cybersecurity maturity in the human resources domain of Bank Indonesia was assessed using the Cybersecurity Capability Maturity Model (C2M2) framework, with findings indicating that key workforce-related areas had not reached maturity level 3, suggesting institutional gaps in capability development [31]. Compliance attitude, in turn, impacts cybersecurity awareness, which impacts intention towards ISPC, and ultimately impacts employee protective action. Overall security outcomes are driven by a cycle of attitude, awareness, and conduct, as shown by this interaction. Although there is a wealth of literature on people's perspectives on cybersecurity, there is a dearth of data on how these perspectives alter across various business models, especially when it comes to SMEs. Thus, this study's fourth, fifth, and sixth hypotheses are: "H4: Cybersecurity awareness is positively associated with cybersecurity compliance attitude". "H5: Cybersecurity compliance attitude is positively associated with intention towards ISPC". "H6: Cybersecurity compliance attitude is positively associated with employee protective behavior".

2.9 Information protection motivation

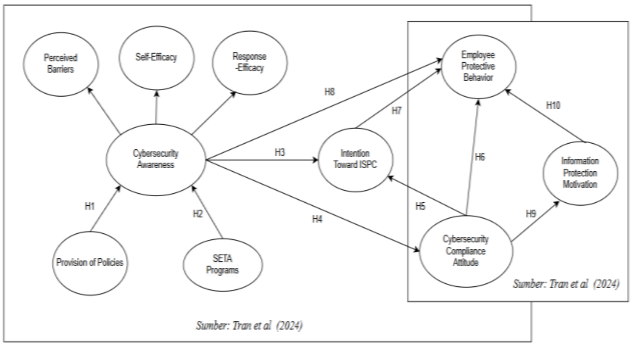
One way to get more people to follow security rules is to incentivize them to keep sensitive information safe. Individuals are motivated to take essential activities to prevent security breaches when they have strong protection motive, according to Rogers [18]. According to references [32, 33], employees with a strong commitment to protecting sensitive information are more likely to engage in proactive behaviors that help reduce the risk of cyberattacks. Organizations need this incentive to foster a culture of compliance and encourage effective protective behaviors [34]. In the Protection Motivation Theory (PMT), individual motivation to protect information is influenced by cognitive evaluations, including attitudes toward protective behaviors [35]. When employees perceive compliance with cybersecurity policies positively, this favorable attitude can strengthen their perceived value and necessity of engaging in protective actions, thereby enhancing their motivation to protect information [36]. Additionally, in attitude-behavior models like the Theory of Planned Behavior (TPB), attitude serves as an antecedent to both intention and motivational factors driving behavior [17]. Therefore, a positive cybersecurity compliance attitude can be expected to enhance information protection motivation. Since this is the case, testable hypotheses nine and ten are: "H9: Cybersecurity compliance attitude is positively associated with Information protection motivation".

2.10 Employee protective behavior

The term "employee protective behavior" describes the measures taken by workers to safeguard data and lessen possibilities of cyberattacks. According to research by Johnston and Warkentin [37], Employees tend to follow protective practices when they feel confident they can maintain workplace security. When employees are aware of the repercussions of policy noncompliance, they are more likely to act protectively, as Tsohou et al. [38] pointed out. By examining how employee cybersecurity behaviors can be improved through the interaction of awareness, policies, and compliance attitudes, this study hopes to fill a vacuum in the existing literature on cybersecurity and help create a safer workplace environment. The purpose of this study is to provide practical suggestions for improving organizational cybersecurity strategies by testing hypotheses and offering fresh insights into the relationships between cybersecurity awareness, compliance attitudes, and protective behaviors. Since this is the case, testable hypotheses seven and eight are: "H7: Intention towards ISPC is positively associated with employee protective behavior". "H8: Cybersecurity awareness is positively associated with employee protective behavior". "H10: Information protection Motivation is positively associated with Employee protective behavior".

3. THORETICAL FRAMEWORK AND HYPOTHESES

This study delves at the knowledge and actions of employees about information security at Indonesia's biggest bank. This study fills a gap in the literature by expanding on prior work that focused on six critical aspects impacting information security practices: policy provision, SETA programs, cybersecurity awareness, intention toward ISPC, cybersecurity compliance attitude, and employee protective behavior. In order to provide a more complete and nuanced picture of the factors that influence information security behavior, this study combines results from two other investigations. "From awareness to behaviour: understanding cybersecurity compliance in Vietnam" and "Exploring the influence of government social media on cybersecurity compliance: employee attitudes, motivation, and behaviors" are two studies that look at different aspects of the topic. The first study examines how people in Vietnam feel about cybersecurity and how that relates to their attitudes and behaviors when it comes to compliance [16, 29]. Information protection motivation is one of seven factors that our study found to have a direct impact on whether workers engage in protective security measures. This study builds a more comprehensive framework by combining these observations, which helps us understand the factors that influence employee security behavior better. The study's conceptual framework is shown in Figure 1.



Sumber: Tran et al (2024)

Sumber: Tran et al (2024)

Figure 1. Framework model

This paper elaborates on seven key dimensions of information security awareness and behavior, enhancing the framework in Figure 1 and grounded in previous theoretical work. Hence, the following are the research hypotheses:

“H1: Provision of policies is positively associated with cybersecurity awareness.”

“H2: SETA programs are positively related to cybersecurity awareness.”

“H3: Cybersecurity awareness is positively associated with intention towards ISPC.”

“H4: Cybersecurity awareness is positively associated with cybersecurity compliance attitude.”

“H5: Cybersecurity compliance attitude is positively associated with intention towards ISPC.”

“H6: Cybersecurity compliance attitude is positively associated with employee protective behavior.”

“H7: Intention towards ISPC is positively associated with employee protective behavior.”

“H8: Cybersecurity awareness is positively associated with employee protective behavior.”

“H9: Cybersecurity compliance attitude is positively associated with Information protection motivation.”

“H10: Information protection motivation is positively associated with Employee protective behavior.”

The information security awareness and behavior were assessed in this study using a structured questionnaire that was derived from earlier literature [16, 29]. The validity and reliability assessments were carried out using SPSS with 30 respondents, which met the minimum requirement for testing, prior to full-scale implementation. To ensure that each measurement item accurately reflected the target construct, validity was determined by checking that the item's correlation coefficient (r-count) was greater than the crucial table value (r-table). Using Cronbach's alpha, a widely recognized indication of internal consistency, the instrument's dependability was assessed. According to Hair et al. [39], a statistically reliable coefficient is one that is equal to or greater than 0.70. To get to people's opinions, the survey used a five-point Likert scale, where 1 means strongly disagree and 5 means strongly agree. Applying Slovin's calculation with a 5% margin of error, we were able to calculate that 315 responses were the minimum required for the sample size. The results are more likely to be accurate because this method guarantees statistical robustness and representativeness.

Table 1. Key characteristics of respondents

	Category	*n*=360	%
Gender	Male	188	52.22%
	Female	172	47.78%
Age	Boomer Generation	1	0.28%
	Generation X	45	52.78%
	Generation Y/Millennials	190	34.44%
	Generation Z	124	12.50%
Education level	Doktor	1	0.28%
	S2 Magister	32	8.89%
	D4/S1	246	68.33%
	D3	31	8.61%
	SMA/SMK/SLTA	49	13.61%
	SMP/SLTP	1	0.28%
Years of experience	0-1 tahun	36	10%
	2-3 tahun	99	27.50%
	4-5 tahun	62	17.22%
	>5 tahun	163	45.28%
Income per month	<1.000.000	12	3.33%
	1.000.000-5.000.000	127	35.28%
	5.000.000-10.000.000	145	40.28%
	10.000.000-15.000.000	58	16.11%
	>15.000.000	27	7.50%

A total of 360 respondents participated in this study, all of whom worked for Indonesia's three biggest state-owned banks, filled out the survey. According to Table 1, which shows the important demographic features of the sample, 188 (52.22%) were male and 172 (47.78%) were female of the respondents. Generation Z accounted for 34.44% of the participants, suggesting an overwhelmingly younger workforce, while Generation Y/Millennials accounted for 52.78%. The educational history of the respondents reveals a rather high level of accomplishment, with the highest proportion holding a D4/S1 degree (68.33%) and those with SMA/SMK/S LTA education (13.61%) following closely behind. When asked about their length of service at the bank, 45.28 percent of respondents had been there for five years or more, with 17.22 percent having four to five years of experience. This suggests that the staff has extensive expertise in the banking industry. The selection procedure for this investigation was the probability sampling method. Additionally, the data were examined by employing the PLS-SEM approach (Partial Least Squares-Structural Equation Modeling). A bootstrapping procedure with 5000 resamples was conducted to enhance the robustness of the analysis stronger. To verify the reliability of the data, we tested our hypotheses by analyzing the P and T values.

4. DATA AND METHODOLOGY

4.1 Responses analysis

The survey results disclose significant information regarding employees' perceptions of the company's policies under the provision of policies variable. Table 2 shows that although many employees concur with company policies, there are clear deficiencies in comprehension or implementation. The highest percentage of Strongly Disagree responses was recorded for the statement prohibiting unauthorized access to documents stored on computers (PP3), with 2.78% strongly disagreeing, while the highest Disagree response appeared for internal computer use standards (PP2), with 8.89% disagreeing. The highest Neutral response was found in the statement about general computer-use conduct (PP1), at 13.89%, possibly indicating uncertainty. On the other hand, PP2 received the most Agree responses at 30%, and the highest Strongly Agree responses were recorded for the statement "My company has a code of ethics that outlines guidelines on information security, and every employee is expected to comply with these rules" (PP4), with 61.67% strongly agreeing. These results suggest a generally positive view of policy provisions, though further efforts are needed to improve awareness and consistent implementation.

Table 2. Provision of policies-related responses

Statements on Questionnaires Related to Provision of Policies	Reference	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
"My company has established rules of conduct for computer use in accordance with applicable regulations. (PP1)"	[16]	0.56%	4.44%	13.89%	28.33%	52.78%
"My company has guidelines for the use of computers within the company that are in accordance with applicable regulations. (PP2)"		0.56%	8.89%	7.78%	30%	52.78%
"The Company establishes a policy to restrict unauthorized employees from viewing or retrieving computer-based documents, in accordance with applicable regulations. (PP3)"		2.78%	8.33%	7.78%	22.78%	58.33%
"My company has a code of conduct that outlines guidelines on information security, and every employee is expected to abide by these rules. (PP4)"		0.56%	5.56%	12.78%	19.44%	61.67%

Table 3. SETA programs-related responses

Statements on Questionnaires Related to SETA Programs	Reference	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
"My company often conducts briefings on security breach topics through information security awareness (email, brochures/seminars/workshops). (SETA1)"	[16]	0.56%	7.22%	11.11%	32.78%	48.33%
"My company routinely shares information about emerging cyber threats and recommended protective measures for myself. (SETA2)"		1.11%	6.67%	11.67%	30%	50.56%
"My company provide ongoing training to staff members on their role in maintaining computer security. (SETA3)"		1.11%	6.67%	14.44%	32.78%	45%
"Cybersecurity awareness training conducted by my company is designed with comprehensive information on cybersecurity threats. (SETA4)"		1.11%	7.22%	16.67%	23.33%	51.67%
"Awareness initiatives related to cybersecurity within my company enable me to acquire the skills needed for carrying out safeguarding behaviors. (SETA5)"		1.11%	6.11%	13.33%	31.11%	48.33%

Furthermore, Table 3 indicates that employees generally recognize the merit of SETA programs; nevertheless, there remains potential for improvement in their execution. The highest percentage of Strongly Disagree responses was recorded across four statements—SETA2, SETA3, SETA4, and SETA5—each with 1.11%, while the highest Disagree responses appeared for the statements about security breach briefings (SETA1) and cybersecurity education sessions (SETA4), both with 7.22%. The highest percentage of Neutral responses was recorded for the statement regarding cybersecurity education sessions at the company (SETA4), with 16.67% remaining neutral, suggesting uncertainty about the content or delivery of such sessions. The highest percentage of Agree responses was found in the statements on SETA1 and SETA3, both at 32.78%. Meanwhile, the highest percentage of Strongly Agree responses was observed in the statement SETA4, with 51.67% strongly agreeing, indicating that a significant number of employees appreciate the depth of these programs. These findings show that while SETA programs exert a positive influence, enhancing their consistency and clarity remains essential to optimize their impact.

The survey results offer insights into employees' assessments of response efficacy and their confidence in security processes. Table 4 shows that the highest percentage of Strongly Disagree responses was recorded for RE1 and RE3, each at 1.11%, while the highest Disagree response was found in RE1 at 7.22%, indicating some concern regarding confidentiality safeguards. The highest Neutral responses were noted in RE2, with 38.33% expressing uncertainty about protection from breaches. The highest Agree response was recorded for RE9 at 51.11%, and the highest Strongly Agree response appeared in RE6, at 36.11%, showing trust in policy compliance to reduce threats. While overall trust in response efficacy is evident, further training and practical examples remain necessary to improve understanding.

Table 5 indicates that employees predominantly possess confidence in their capacity to safeguard information. The highest percentage of Strongly Disagree responses was recorded for the statements "I am confident in my ability to protect myself from security information breaches (SE4)" and "I trust my competence in managing virus-infected files effectively (SE6)," both at 3.33%. The statement SE7 received the highest percentage of Disagree responses, at 13.33%. The highest percentage of Neutral replies was also found in SE7, at 24.44%. For the Agree category, the highest percentage was observed for SE1 and SE2 both at 32.78%. The Strongly Agree response was most prominent for "My practice includes utilizing protective measures, such as firewalls and antivirus software, on the computers I use for work. (SE3)," at 55.56%. These findings reflect a considerable level of self-assurance among employees; however, the variation in responses—particularly regarding more technical tasks—suggests a need for continuous and practical training to enhance the effective use of information security measures.

Table 4. Response efficacy-related responses

Statements on Questionnaires Related to Response Efficacy	Reference	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
"My company has implemented effective measures to protect my confidential information. (RE1)"	[16]	1.11%	7.22%	21.11%	37.78%	32.78%
"My work information is well protected from security breaches through the security measures implemented at my company. (RE2)"		0%	6.11%	38.33%	37.78%	17.78%
"In my company, there are effective safeguards in place to prevent the spread of harmful information. (RE3)"		1.11%	6,11%	28.33%	40%	24.44%
"My company implements protective measures to block unauthorized access to systems that hold confidential data and personal details. (RE4)"		0%	3.33%	31.11%	33.33%	32.22%
"Potential security risks can be minimized when I adhere to my organization's information security policy. (RE5)"		0%	4.44%	28.33%	38.89%	28.33%
"The chance of a cybersecurity breach is expected to decline when I comply with current data protection guidelines. (RE6)"		0%	5%	15.56%	43.33%	36.11%
"Potential security problems may be avoided by adhering to a disciplined information security policy. (RE7)"		0%	6.11%	21.11%	38.89%	33.89%
"My company enhances information security by providing concrete examples of the use of cybersecurity practices. (RE8)"		0%	6.67%	25%	45.56%	22.78%
"Antivirus and firewall software upgrades are considered very important to maintain information security. (RE9)"		0%	1.67%	19.44%	51.11%	22.78%

Table 5. Self-efficacy-related responses

Statements on Questionnaires Related to Self-Efficacy	Reference	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
"I believe that I have sufficient skills to protect information from security breaches. (SE1)"	[16]	1.11%	5.56%	12.78%	32.78%	47.78%
"I believe that I can maintain the privacy of my information by taking personal responsibility. (SE2)"		1.11%	6.11%	12.78%	32.78%	47.78%
"My practice includes utilizing protective measures, such as firewalls and antivirus software, on the computers I use for work. (SE3)"		0.56%	7.22%	14.44%	22.22%	55.56%
"I am confident in my ability to protect myself from security information breaches. (SE4)"		3.33%	8.89%	15%	28.33%	44.44%
"I feel comfortable customizing the security level in the web browser I use. (SE5)"		1.67%	0.10%	13.33%	25.56%	49.44%
"I trust my competence in managing virus-infected files effectively. (SE6)"		3.33%	0.10%	23.33%	27.22%	36.11%
"I am confident in my ability to remove malicious software or malware from my computer. (SE7)"		1.67%	13.33%	24.44%	28.89%	31.67%

Table 6. Perceived barriers-related responses

Statements on Questionnaires Related to Perceived Barriers	Reference	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
"I feel uncomfortable when having to verify emails with attached files. (PB1)"	[16]	13.33%	17.78%	29.44%	24.44%	15%
"I feel uncomfortable when I need to make changes to personal settings on social media platforms. (PB2)"		13.33%	19.44%	29.44%	21.67%	16.11%
"I feel uncomfortable backing up computer data regularly. (PB3)"		18.33%	24.44%	25%	18.33%	13.89%

Table 7. Intention toward ISPC-related responses

Statements on Questionnaires Related to Intention Toward ISPC	Reference	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
"My goal is to safeguard data assets and technological systems following the company's established information security guidelines. (ISPC1)"	[16]	1.11%	5.56%	14.44%	29.44%	49.44%
"Going forward, I plan to adhere to the regulations outlined within the company's cybersecurity policy. (ISPC2)"		0.56%	4.44%	13.33%	32.22%	49.44%
"Going forward, I plan to carry out tasks related to information security policies. (ISPC3)"		0.56%	8.89%	15.56%	28.89%	46.11%
"I intend to comply with the information security policies implemented by the company. (ISPC4)"		111%	5.56%	16.67	26.67%	50%

Table 8. Cybersecurity compliance attitude-related responses

Statements on Questionnaires Related to Cybersecurity Compliance Attitude	Reference	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
"I feel that complying with the information security policy in my company is very important. (ATT1)"	[16]	0.56%	6.67%	14.44%	22.78%	55.56%
"I am confident that I am capable of complying with applicable information security policies. (ATT2)"		0.56%	6.11%	15.56%	25.56%	52.22%
"I agree that following the information security policy in my company is advisable. (ATT3)"		0.56%	8.33%	11.67%	23.89%	55.56%

Table 6 delineates obstacles perceived by employees in implementing cybersecurity measures. The highest percentage of Strongly Disagree responses was recorded for the statement "I feel uncomfortable backing up computer data regularly (PB3)," with 18.33%, while the highest percentage of Disagree responses was also found in PB3, at 24.44%. The highest percentage of Neutral replies was observed for the statements "I feel uncomfortable when having to verify emails with attached files (PB1)" and "I feel uncomfortable when I need to make changes to personal settings on social media platforms (PB2)," both at 29.44%. In the Agree category, the highest percentage was found in PB1, at 24.44%. Similarly, the highest percentage of Strongly Agree responses was also seen in PB1, at 15%. These findings suggest that while discomfort in certain technical tasks such as data backup and settings modification persists, email verification remains the most prominent source of perceived difficulty, underscoring the need for targeted interventions to reduce apprehension and improve task familiarity.

Table 7 assesses employees' intentions to adhere to information security policies. The highest percentage of Strongly Disagree responses was recorded for the statements "My goal is to safeguard data assets and technological systems following the company's established information security guidelines (ISPC1)" and "I intend to comply with the information security policies implemented by the company (ISPC4)," both at 1.11%, while the highest Disagree response was found in "Going forward, I plan to carry out tasks related to information security policies (ISPC3)," at 8.89%. The highest percentage of Neutral replies was recorded for ISPC3, with 15.56%. For the Agree category, the highest percentage was seen in "Going forward, I plan to adhere to the regulations outlined within the company's cybersecurity policy (ISPC2)," at 32.22%. The highest percentage of Strongly Agree responses was found in ISPC4, at 50%. These findings indicate a strong intention among employees to comply with the organization's information security policies; nonetheless, consistent reinforcement through training and clear policy communication remains essential to ensure the actualization of these intentions into compliant behavior.

Table 8 examines employees' perspectives on cybersecurity compliance. The highest percentage of Strongly Disagree responses was consistent across all items at 0.56%, while the highest Disagree response was recorded for "I agree that following the information security policy in my company is advisable (ATT3)," at 8.33%. The highest percentage of Neutral replies appeared in "I am confident that I am capable of complying with applicable information security policies (ATT2)," with 15.56%. In the Agree category, the highest response was observed for ATT2, at 25.56%. For the Strongly Agree category, the highest percentage was found in both ATT1 and ATT3, each with 55.56%. These findings suggest that employees generally hold positive attitudes toward cybersecurity compliance, with strong confidence and agreement toward policy importance and feasibility; however, regular training and policy engagement efforts remain essential to reinforce these favorable attitudes into sustained behavioral compliance.

Table 9 evaluates employees' motivation to safeguard information. The highest percentage of Strongly Disagree responses was consistently recorded at 1.11% across four of the five statements, while the highest Disagree response was found in "I am committed to making every effort necessary to protect my company from information security risks (IPM4)," at 8.89%. The highest percentage of Neutral replies was observed for "I am determined to take all necessary measures to prevent information security threats from occurring in my company (IPM5)," at 14.44%. For the Agree category, the highest percentage was noted for IPM4, at 29.44%. The highest Strongly Agree response was found in "I am committed to protecting my company from information security risks (IPM1)," at 56.67%. These results indicate a high level of motivation among employees to protect information assets; nevertheless, to translate this motivation into sustained protective actions, structured guidance and clearly defined procedural steps should be emphasized.

Table 10 emphasizes genuine protective activities. The highest percentage of Strongly Disagree responses was noted for "I have observed abnormal behavior on my device (such as the system becoming slow, freezing, or unexpected windows appearing)." (EPB2), at 3.33%, while the highest Disagree percentage was also from EPB2, at 10%. The Neutral responses peaked at 18.33% and were shared across all two statements, indicating a common level of uncertainty or passive behavior among respondents. The highest percentage of Agree responses was recorded for EPB2, at 30%. The highest Strongly Agree response was found for "My computer is consistently protected with the latest antivirus updates" (EPB1), at 45%. These findings reflect that while many employees exhibit proactive behavior in certain protective practices, such as responding to malware alerts, more deliberate efforts and targeted reinforcement are necessary to encourage consistent and comprehensive protective behavior.

Table 9. Information protection motivation-related responses

Statements on Questionnaires Related to Information Protection Motivation	Reference	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
"I am committed to protecting my company from information security risks. (IPM1)"	[29]	1.11%	6.67%	11.11%	24.44%	56.67%
"I have a strong intention to prevent information security threats to my company. (IPM2)"		1.11%	6.11%	13.33%	25%	54.44%
"I will take measures to protect my company's information and information systems from security threats. (IPM3)"		1.11%	8.33%	12.22%	24.44%	53.89%
"I am committed to making every effort necessary to protect my company from information security risks. (IPM4)"		0.56%	8.89%	7.78%	29.44%	53.33%
"I am determined to take all necessary measures to prevent information security threats from occurring in my company. (IPM5)"		1.11%	6.11%	14.44%	24.44%	53.89%

Table 10. Employee protective behavior-related responses

Statements on Questionnaires Related to Employee Protective Behavior	Reference	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
"My computer is consistently protected with the latest antivirus updates. (EPB1)"	[16]	2.78%	6.67%	17.78%	27.78%	45%
"I have observed abnormal behavior on my device (such as the system becoming slow, freezing, or unexpected windows appearing). (EPB2)"		3.33%	10%	18.33%	30%	38.33%
"I react promptly to any malware alerts that arise. (EPB3)"		2.22%	7.78%	18.33%	29.44%	42.22%

The analysis of responses in this study was carried out by converting quantitative mean scores into qualitative categories to facilitate interpretation. This categorization follows the approach proposed by Pimentel [40] and Boone and Boone [41], who recommend dividing the five-point Likert scale into five equal intervals. According to these authors, values ranging from 4.21 to 5.00 are categorized as Very Good, values from 3.41 to 4.20 are categorized as Good, values from 2.61 to 3.40 are categorized as Normal, values from 1.81 to 2.60 are categorized as Poor, and values from 1.00 to 1.80 are categorized as Very Poor. This method is widely used in behavioral and educational research to interpret Likert scale data, particularly when assessing attitudes, behaviors, and perceptions. In this study, the mean scores of each measured variable were mapped onto these categories to evaluate the extent of cybersecurity compliance practices among employees [40, 41].

Table 11. Average of responses per variable

Variables	PP	SETA	SE	RE	PB	ISPC	ATT	IPM	EPB
Mean Score	4.28	4.19	3.97	3.94	3.02	4.47	4.11	4.36	3.99
Category	Very Good	Good	Good	Good	Normal	Very Good	Good	Very Good	Good

As shown in Table 11, one of the biggest state-owned banks in Indonesia, Bank X, had average replies across multiple dimensions of cybersecurity compliance. The table summarizes the results by classifying the mean scores of each variable according to the degree of information security awareness and compliance among the employees. Scores on the variables indicate general security understanding, behaviors, and perceptions; they range from Very Good to Normal.

With an average score of 4.47, falling into the Very Good category, Intention towards ISPC (ISPC) comes out on top in Table 11. This shows that Bank X staff are very concerned about protecting customer data and are aware that their activities have an impact on the probability of cybercrime. The provision of policies (PP) component also received a high score, averaging 4.28 and falling into the Very Good category. This indicates that Bank X's security policy is well-defined, well-organized, and widely known by staff members, helping them to understand their specific duties in safeguarding the company's data. Bank X's security training program achieved a Good SETA program score of 4.19, indicating effectiveness, yet there is room for improvement in consistent application among employees. Despite a Good cybersecurity compliance attitude (ATT) score of 4.11, and an Excellent Information Protection Motivation (IPM) score of 4.36, inconsistent adherence to security practices persists. The Perceived Barrier (PB) score of 3.02 (Normal) highlights the gap between awareness and action, suggesting that employees recognize the importance of security but may find compliance burdensome. Similarly, the Self-Efficacy (SE) and Response Efficacy (RE) scores of 3.94 and 3.97 (Good) reflect awareness but not consistent behavior.

Addressing the Perceived Barrier is crucial to reduce the perceived complexity and costs associated with cybersecurity measures. Strengthening proactive risk assessment, environmental security management, and continuous training reinforcement can help bridge the gap between awareness and consistent practice. Without these efforts, high awareness alone is insufficient to achieve full compliance.

4.2 Validity and reliability testing

The validity and reliability of the constructs were examined in this study by testing the measurement model, also known as the outer model. Discriminant validity is checked using the Fornell-Larcker criterion, which checks that the value of each construct is greater than its correlation with other variables [42]. All of the model's variables satisfy the validity requirements, as shown in Table 12. Discriminant validity is demonstrated when the value of each variable exceeds its correlation with other variables.

Table 12. Fornell-Larcker criterion test results

	ATT	EPB	IPM	ISPC	PB	PP	RE	SETA	SE
ATT	0.935								
EPB	0.831	0.909							
IPM	0.900	0.820	0.938						
ISPC	0.885	0.815	0.896	0.925					
PB	0.297	0.399	0.332	0.286	0.899				
PP	0.837	0.768	0.865	0.823	0.279	0.902			
RE	0.073	0.079	0.070	0.053	0.170	0.052	0.745		
SETA	0.793	0.818	0.856	0.825	0.352	0.868	0.031	0.894	
SE	0.816	0.795	0.828	0.807	0.401	0.817	0.082	0.844	0.867

Table 13. Reliability and construct validity test results

	Cronbach 's Alpha	Composite Reliability (rho_a)	Composite Reliability (rho_c)	(AVE)
ATT	0.928	0.930	0.954	0.874
EPB	0.895	0.898	0.935	0.827
IPM	0.966	0.966	0.974	0.881
ISPC	0.944	0.945	0.960	0.856
PB	0.882	0.917	0.926	0.808
PP	0.923	0.924	0.946	0.814
RE	0.913	1.097	0.918	0.555
SETA	0.937	0.939	0.952	0.800
SE	0.945	0.952	0.955	0.751

To evaluate the validity and reliability of the constructs, this study employed additional statistical indicators including Cronbach's alpha, composite reliability, and the average variance extracted (AVE). According to existing literature, a construct is deemed valid when the AVE value surpasses 0.5, and both Cronbach's alpha and composite reliability meet or exceed the threshold of 0.6 [42]. These results affirm that the measurement model used in this study is both valid and reliable, which is essential for ensuring the credibility and accuracy of the research findings. Based on the results presented in Table 13 and Figure 2, it can be concluded that the constructs are statistically sound and dependable.

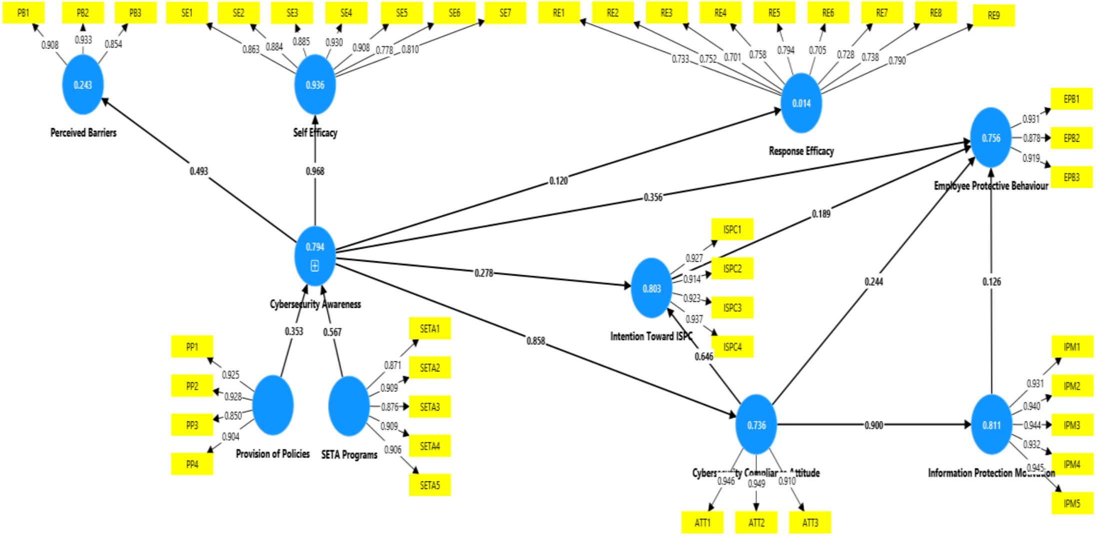


Figure 2. Output results of outer loading values

Table 14. Output result of path coefficients

Hypothesis	Original Sample	Sample Mean	Standard Deviation	T Statistics	P Value	Result
PP→CSA	0.353	0.359	0.061	5.798	0.000	significant
SETA→CSA	0.567	0.563	0.059	9.579	0.000	significant
CSA→ISPC	0.278	0.292	0.065	4.270	0.000	significant
CSA→ATT	0.858	0.862	0.018	46.927	0.000	significant
ATT→ISPC	0.646	0.633	0.061	10.588	0.000	significant
ATT→EPB	0.244	0.234	0.080	3.064	0.001	significant
ISPC→EPB	0.189	0.181	0.060	3.150	0.001	significant
CSA→EPB	0.356	0.372	0.075	4.750	0.000	significant
ATT→IPM	0.900	0.900	0.014	62.483	0.000	significant
IPM→EPB	0.126	0.129	0.104	1.208	0.114	Not significant

4.3 Structural model (inner model)

Table 14 displays the path coefficients employed to analyze the links among latent constructs in this research. The criterion for significance are a T-statistic over 1.96 and a P-value below 0.05. The results demonstrate substantial correlations among the majority of variables, with the exception of the correlation between IPM and EPB. In particular:

- The path coefficient from provision of policies (PP) to cybersecurity awareness (CSA) is 0.353 (T = 5.798, $p < 0.001$), signifying a substantial link between the two variables.
- SETA → CSA exhibits a path coefficient of 0.567 (T = 9.579, $p < 0.001$), indicating a strong impact of security training and awareness (SETA) on CSA.
- The path coefficient between cybersecurity awareness (CSA) and cybersecurity compliance attitude (ATT) is 0.858 (T = 46.927, $p < 0.001$), signifying a highly significant link.
- ATT significantly affects ISPC (0.646, $p < 0.001$) and EPB (0.244, $p < 0.001$), indicating a strong relationship between cybersecurity compliance attitude and Intention toward ISPC as well as employee protective behavior.
- The relationship between information protection motivation (IPM) and employee protective behavior (EPB) is not significant (0.126, $p = 0.114$), as seen by a T-statistic of 1.208 and a P-value beyond 0.05, showing that IPM does not significantly affect EPB. Consequently, personnel at Bank X must cultivate a more robust favorable disposition towards cybersecurity to enhance personal protection motivation, thereby resulting in greater adherence to current cybersecurity protection regulations.

The two most substantial route coefficients are CSA → ATT (0.858) and ATT → IPM (0.900). The elevated path coefficient of ATT → IPM signifies that cybersecurity compliance attitude (ATT) substantially affects information protection motivation (IPM), thereby improving adherence to cyberspace protection rules.

4.4 Hypothesis discussion

4.4.1 The provision of policies is positively associated with cybersecurity awareness

The findings corroborate H1, indicating a substantial positive correlation between policy provision and cybersecurity awareness ($\beta = 0.353$, $p < 0.05$). This research indicates that robust cybersecurity regulations at Bank X enhance workers' awareness of security measures. This aligns with other research, which has shown that explicit policies improve employees' comprehension and adherence to cybersecurity protocols [16, 43]. The evidence suggests that this policy provision is a critical factor in enhancing cybersecurity awareness, solidifying its status as a fundamental ingredient for behavioral change.

4.4.2 SETA programmes are positively related to cybersecurity awareness

The analysis indicates that H2 is corroborated, exhibiting a substantial route coefficient ($\beta = 0.567$, $p < 0.05$). This suggests that SETA (Security Education, Training, and Awareness) programs are positively associated with cybersecurity awareness. This outcome aligns with previous studies indicating that instructional interventions, such as SETA programs, effectively enhance employees' cybersecurity awareness [16, 44]. These programs seem to be a crucial instrument in alleviating the risks associated with human error in cybersecurity, along with the global trend of employing continuous education to enhance cybersecurity preparedness.

4.4.3 Cybersecurity awareness is positively related with intentions towards ISPC

The findings for H3 reveal a moderate but substantial positive correlation ($\beta = 0.244$, $p < 0.05$) between cybersecurity awareness and intentions toward ISPC. This corroborates the hypothesis that awareness affects employees' intention to adhere to information security standards. Prior research substantiates this correlation, indicating that heightened knowledge fosters more proactive compliance attitudes [16]. Consequently, augmenting awareness may improve employees' intention to comply with ISPC, thereby fostering superior overall compliance rates.

4.4.4 Cybersecurity awareness is positively associated with compliance attitudes

The results for H4 demonstrate a significant correlation ($\beta = 0.646$, $p < 0.05$), suggesting that cybersecurity knowledge is positively linked to compliance attitudes. This corresponds with research highlighting that increased understanding fosters more positive attitudes towards compliance with security policies [16, 43]. The findings indicate that improving awareness of security threats may enhance employees' compliance attitudes and, thus, strengthen the organizational security culture.

4.4.5 Cybersecurity compliance attitude is positively related with intentions towards ISPC

H5 demonstrates a notable positive correlation ($\beta = 0.244$, $p < 0.05$) between compliance attitude and intention toward ISPC. This indicates that personnel with favorable attitudes toward cybersecurity are more inclined to demonstrate intent to adhere to information security standards. Prior research corroborates this conclusion, indicating that a favorable security compliance disposition is a robust predictor of actual compliance behavior [16].

4.4.6 Cybersecurity compliance attitude is positively related with employee protective behavior

Hypothesis 6 substantiates that compliance attitudes substantially affect protective conduct ($\beta = 0.189$, $p < 0.05$), suggesting that employees with favorable compliance attitudes are more inclined to exhibit protective behavior. This aligns with current literature, indicating that a proactive approach to security typically results in enhanced protective measures, including password management and secure data handling [16].

4.4.7 Intention towards ISPC is positively related with employee protective behavior

The findings for H7 demonstrate a substantial correlation ($\beta = 0.900$, $p < 0.05$), suggesting that employees' intention to adhere to ISPC is closely associated with protective conduct. This aligns with other studies indicating a clear correlation between compliance intention and the preventative measures undertaken by employees [16]. This emphasizes the significance of cultivating compliance intentions to affect practical protective behavior.

4.4.8 Security awareness is positively associated with employee protective behavior

Hypothesis 8 is substantiated by a substantial path coefficient ($\beta = 0.858$, $p < 0.05$). Cybersecurity awareness is essential in fostering protective behavior among employees. This discovery corresponds with previous research highlighting the impact of security risk awareness on the implementation of preventative strategies [26]. The findings indicates that heightened awareness is a crucial element in fostering secure practices at the individual level.

4.4.9 Cybersecurity compliance attitudes is positively associated with information protection motivation

The findings for H9 reveal a significant path coefficient ($\beta = 0.633$, $p < 0.05$), indicating that a good compliance attitude towards cybersecurity correlates with enhanced motivation to safeguard information. This aligns with literature that associates compliance with intrinsic incentive for sustaining security [29, 32]. It emphasizes that employees who perceive compliance as a beneficial action are more inclined to actively safeguard sensitive information.

4.4.10 Information protection motivation is positively associated with employee protective behavior

The H10 analysis results indicated a weak but significant correlation ($\beta = 0.126$, $p < 0.05$) between information protection motivation and employees' protective conduct. Although Information Protection Motivation (IPM) showed a positive relationship with Employee Protective Behavior (EPB), this effect was not significant, indicating a gap between motivation and protective action. In a collective and hierarchy-oriented culture like Indonesia, employees tend to wait for formal directives or follow group norms instead of taking initiative, so IPM does not automatically translate into action [45]. In addition, psychological factors such as self-efficacy and response efficacy may mediate this relationship; when individuals do not believe that their actions are effective or feel a lack of confidence, they tend to be passive despite their motivation [46]. Therefore, the effectiveness of IPM is highly dependent on contextual supports such as organizational culture, work culture in Indonesia, threat awareness, and adequate training structures. The variance in results is likely attributable to the characteristics of the respondents in this study. Awareness of cybersecurity hazards in this sector is inadequate, emphasizing formal security policies above proactive defensive strategies. Furthermore, the hierarchical company culture promotes compliance with processes while neglecting individual safeguarding. This differs from other research in Vietnam, which encompassed sectors with elevated awareness levels and cultures that more effectively endorse information protection motivation [29]. This elucidates the diminished correlation between personal protective motivation and employee protective conduct within the Indonesian banking sector.

5. CONCLUSIONS

This study seeks to examine the influence of workers' cybersecurity understanding and activities on their protective attitudes toward information security at Bank X in Indonesia. The findings of this study highlight that the most critical driver in shaping employees' protective behavior is their attitude toward cybersecurity compliance. This is evidenced by the strong and significant relationship between cybersecurity compliance attitude and information protection motivation and between cybersecurity awareness and compliance attitude. These results suggest that employee attitude serves as a central psychological lever in transforming awareness into intrinsic motivation and concrete protective behavior. Therefore, organizations, particularly in the banking sector, are encouraged to not only increase employees' awareness through SETA programs but also ensure these interventions are designed to influence attitudes—such as by embedding emotional engagement, real-life case studies, and positive framing around security compliance. Enhancing employee attitudes toward cybersecurity will significantly boost their internal motivation and the likelihood of adopting secure behaviors, making attitude cultivation a strategic priority in cybersecurity policy implementation.

Banks are advised to continue strengthening the provision of clear and comprehensive cybersecurity policies and to regularly conduct cybersecurity training programs for all employees. Effective training programs can increase employee awareness and compliance with cybersecurity, thereby encouraging better protective intentions and behaviors in protecting information systems. In addition, periodic evaluation of policies and training is essential to adapt to the ever-evolving dynamics of cyber threats. A holistic and sustainable approach will help build a strong cybersecurity culture in the banking environment.

This study does not cover all other important factors that may influence employees' protective behavior, such as protection knowledge, organizational culture, technological support, perceived risk, and social and psychological influences. Therefore, these factors should be taken into account by future researchers when creating a research framework. This study's focus is limited to the financial industry, which may influence the findings. Further research should account for sectoral and national differences to strengthen these findings across various sectors.

ACKNOWLEDGMENT

We extend our gratitude to the respondents who participated in completing the questionnaires and to Telkom University for their invaluable support, particularly for their support in providing useful academic references.

REFERENCES

[1] Stefanovic, N., Barjaktarovic, L., Bataev, A. (2021). Digitainability and financial performance: Evidence from the Serbian banking sector. Sustainability, 13(23): 13461. https://doi.org/10.3390/su132313461

[2] Uddin, M.H., Ali, M.H., Hassan, M.K. (2020). Cybersecurity hazards and financial system vulnerability: A synthesis of literature. Risk Management, 22(4): 239-309. https://doi.org/10.1057/s41283-020-00063-2

[3] Bhagwani, V., Balasinorwala, S., Mumbai, K.J.S.P.V. (2023). Cyber security. Interantional Journal of Scientific Research in Engineering and Management, 7(2). https://doi.org/10.55041/IJSREM17691

[4] Saeed, S., Altamimi, S.A., Alkayyal, N.A., Alshehri, E., Alabbad, D.A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. Sensors, 23(15): 6666. https://doi.org/10.3390/s23156666

[5] Okokpujie, K., Kennedy, C.G., Nnodu, K., Noma-Osaghae, E. (2023). Cybersecurity awareness: Investigating students' susceptibility to phishing attacks for sustainable safe email usage in academic environment (a case study of a Nigerian leading university). International Journal of Sustainable Development and Planning, 18(1): 255-263. https://doi.org/10.18280/ijsdp.180127

[6] Jamil, H., Zia, T., Nayeem, T., Whitty, M.T., D'Alessandro, S. (2025). Human-centric cyber security: Applying protection motivation theory to analyse micro business owners' security behaviours. Information & Computer Security, 33(1): 49-76. https://doi.org/10.1108/ICS-10-2023-0176

[7] Marousis, A. (2021). Cybersecurity training lags, while hackers capitalize on COVID-19. TalentLMS. https://www.talentlms.com/blog/cybersecurity-statistics-survey/.

[8] Hu, S.Q., Hsu, C., Zhou, Z.Y. (2022). Security education, training, and awareness programs: Literature review. Journal of Computer Information Systems, 62(4): 752-764. https://doi.org/10.1080/08874417.2021.1913671

[9] Dhillon, G., Abdul Talib, Y.Y., Picoto, W.N. (2020). The mediating role of psychological empowerment in information security compliance intentions. Journal of the Association for Information Systems, 21(1): 5. https://doi.org/10.17705/1jais.00595

[10] 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

[11] Johri, A., Kumar, S. (2023). Exploring customer awareness towards their cyber security in the Kingdom of Saudi Arabia: A study in the era of banking digital transformation. Human Behavior and Emerging Technologies, 2023(1): 2103442. https://doi.org/10.1155/2023/2103442

[12] Amoh, J.K., Awunyo-Vitor, D., Ofori-Boateng, K. (2021). Customers' awareness and knowledge level of fraudulent acts in electronic banking in Ghana: Evidence from a universal bank. Journal of Financial Crime, 28(3): 870-882. https://doi.org/10.1108/JFC-08-2020-0161

[13] Candiwan, C., Rianda, L.M. (2024). Transactions at your fingertips: Influential factors in information security behavior for mobile banking users. International Journal of Safety and Security Engineering, 14(3): 795-806. https://doi.org/10.18280/ijsse.140312

[14] Arisya, K.F., Ruldeviyani, Y., Prakoso, R., Fadhilah, A.L. (2020). Measurement of information security awareness level: A case study of mobile banking (M-banking) users. In 2020 Fifth International Conference on Informatics and Computing (ICIC), Gorontalo, Indonesia, pp. 1-5. https://doi.org/10.1109/ICIC50835.2020.9288516

[15] Sudirman, B.P., Sari, P.K. (2023). Differences in information security behavior of smartphone users in Indonesia using Pearson's chi-square and post hoc test. International Journal on Advanced Science, Engineering & Information Technology, 13(2): 703-717. https://doi.org/10.18517/ijaseit.13.2.17975

[16] Tran, D.V., Nguyen, P.V., Le, L.P., Nguyen, S.T.N. (2025). From awareness to behaviour: Understanding cybersecurity compliance in Vietnam. International Journal of Organizational Analysis, 33(1): 209-229. https://doi.org/10.1108/IJOA-12-2023-4147

[17] Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2): 179-211. https://doi.org/ https://doi.org/10.1016/0749-5978(91)90020-T

[18] 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

[19] Shaw, R.S., Chen, C.C., Harris, A.L., Huang, H.J. (2009). The impact of information richness on information security awareness training effectiveness. Computers & Education, 52(1): 92-100. https://doi.org/10.1016/j.compedu.2008.06.011

[20] Witte, K. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. Journal of Health Communication, 1(4): 317-342. https://doi.org/10.1080/108107396127988

[21] Warkentin, M., Johnston, A.C., Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. European Journal of Information Systems, 20(3): 267-284. https://doi.org/10.1057/ejis.2010.72

[22] 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

[23] Almansoori, A., Al-Emran, M., Shaalan, K. (2023). Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. Applied Sciences, 13(9): 5700. https://doi.org/10.3390/app13095700

[24] Chan, M., Woon, I., Kankanhalli, A. (2005). Perceptions of information security in the workplace: Linking information security climate to compliant behavior. Journal of Information Privacy and Security, 1(3): 18-41. https://doi.org/10.1080/15536548.2005.10855772

[25] Hwang, I., Wakefield, R., Kim, S., Kim, T. (2021). Security awareness: The first step in information security compliance behavior. Journal of Computer Information Systems, 61(4): 345-356. https://doi.org/10.1080/08874417.2019.1650676

[26] Cram, W.A., D'arcy, J., Proudfoot, J.G. (2019). Seeing the forest and the trees. MIS quarterly, 43(2): 525-554. https://doi.org/10.25300/MISQ/2019/15117

[27] Firdaus, R.A., Rakhmawati, N.A., Samopa, F. (2024). A state-of-the-art review of cyber threat intelligence awareness programs in mitigating bank cyber attacks. In 2024 IEEE International Symposium on Consumer Technology (ISCT), Kuta, Bali, Indonesia, pp. 648-654. https://doi.org/10.1109/ISCT62336.2024.10791139

[28] Wiafe, I., Koranteng, F.N., Wiafe, A., Obeng, E.N., Yaokumah, W. (2020). The role of norms in information security policy compliance. Information & Computer Security, 28(5): 743-761. https://doi.org/10.1108/ICS-08-2019-0095

[29] Tran, D.V., Nguyen, P.V., Nguyen, A.T.C., Vrontis, D., Dinh, P.U. (2024). Exploring the influence of government social media on cybersecurity compliance: employee attitudes, motivation and behaviors. Journal of Asia Business Studies, 18(1): 204-223. https://doi.org/10.1108/JABS-09-2023-0343

[30] 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. International Journal of Information Management, 66: 102520. https://doi.org/10.1016/j.ijinfomgt.2022.102520

[31] Putra, A.P.G., Humani, F., Zakiy, F.W., Shihab, M.R.,

Ranti, B. (2020). Maturity assessment of cyber security in the workforce management domain: A case study in Bank Indonesia. In 2020 International Conference on Information Technology Systems and Innovation (ICITSI), pp. 89-94. https://doi.org/10.1109/ICITSI50517.2020.9264982

[32] Ma, X. (2022). Is professionals' information security behaviors in Chinese IT organizations for information security protection. Information Processing & Management, 59(1): 102744. https://doi.org/10.1016/j.ipm.2021.102744

[33] Liang, H., Xue, Y.L. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the Association for Information Systems, 11(7): 1. https://doi.org/10.17705/1jais.00232

[34] Siponen, M., Mahmood, M.A., Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information & Management, 51(2): 217-224. https://doi.org/10.1016/j.im.2013.08.006

[35] Maddux, J.E., Rogers, R.W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. Journal of Experimental Social Psychology, 19(5): 469-479. https://doi.org/10.1016/0022-1031(83)90023-9

[36] Ng, B.Y., Kankanhalli, A., Xu, Y.C. (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4): 815-825. https://doi.org/10.1016/j.dss.2008.11.010

[37] Johnston, A.C., Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. MIS Quarterly, 34(3): 549-566. https://doi.org/10.2307/25750691

[38] Tsohou, A., Karyda, M., Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. Computers & Security, 52: 128-141. https://doi.org/10.1016/j.cose.2015.04.006

[39] Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E. (2010). Multivariate Data Analysis, 7th ed. New York: Pearson.

[40] Pimentel, J.L. (2010). A note on the usage of Likert Scaling for research data analysis. USM R&D Journal, 18(2):109-112. https://www.researchgate.net/publication/331231816_A_note_on_the_usage_of_Likert_Scaling_for_research_data_analysis.

[41] Boone Jr, H.N., Boone, D.A. (2012). Analyzing likert data. The Journal of Extension, 50(2): 48. https://doi.org/10.34068/joe.50.02.48

[42] Abdillah, W., Hartono, J. (2015). Partial least square (PLS) Alternatif structural equation modeling (SEM) dalam penelitian bisnis. Yogyakarta: Penerbit Andi, 22: 103-150.

[43] Li, L., He, W., Xu, L., Ash, I., Anwar, M., Yuan, X.H. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management, 45: 13-24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

[44] Alyami, A., Sammon, D., Neville, K., Mahony, C. (2023). The critical success factors for Security Education, Training and Awareness (SETA) program effectiveness: A lifecycle model. Information Technology & People, 36(8): 94-125. https://doi.org/10.1108/ITP-07-2022-0515

[45] Triandis, H.C. (2001). Individualism-collectivism and personality. Journal of Personality, 69(6): 907-924. https://doi.org/10.1111/1467-6494.696169

[46] Posey, C., Roberts, T., Lowry, P.B., Courtney, J., Bennett, B. (2011). Motivating the Insider to Protect Organizational Information Assets: Evidence from Protection Motivation Theory and Rival Explanations. In the Dewald Roode Workshop in Information Systems Security 2011, Blacksburg, Virginia, USA, pp. 1-51.