Jurnal Esensi Infokom Vol 10 No. 2 Oktober 2026
e-ISSN: 2828-6707
https://esensijournal.com/index.php/infokom
DOI: 10.55886/infokom.v10i2.538

Evaluation Model of Cybersecurity Awareness Programs, Employee Engagement, and Employee Accountability at Bank XYZ

Naufalarizqa Ramadha Meisa Putra
Department of Informatics Engineering, Universitas Satya Negara Indonesia
Jl. Arteri Pondok Indah No. 11, South Jakarta, INDONESIA
naufalarizqa@usni.ac.id

***Abstract*— The objective of this study is to examine the relationship between the quality of cybersecurity awareness programme, leadership support, cybersecurity culture and employee engagement with employee accountability at Bank XYZ. The study population comprises 16,500 employees. For the sample, 170 questionnaires were distributed and 158 returned; of which 150 were found valid and included for data processing. This is a quantitative study using Likert Scale questionnaire instrument. Data are analysed using Partial Least Squares Structural Equation Modelling (PLS-SEM). The result shows that the quality of the cybersecurity awareness program has a positive and significant impact on employee engagement (β = 0.195; p = 0.014) and employee accountability (β = 0.206; p = 0.010). Employee engagement has a positive and significant impact on employee accountability (β = 0.222; p = 0.008) and partially mediates the effect of program quality on accountability (β = 0.043; p = 0.046). Leadership support has a positive and significant impact on cybersecurity culture (β = 0.566; p < 0.001). Cybersecurity culture has a positive and significant impact on employee engagement (β = 0.265; p = 0.001) and does not have a significant impact on employee accountability (β = 0.092; p = 0.257). The study results show that the quality of the cybersecurity awareness programme influences employee accountability directly and indirectly (through employee engagement), leadership support has a significant effect on the cybersecurity culture.**
Keywords— accountability, cybersecurity awareness, employee engagement, leadership support, PLS-SEM, security culture

Intisari— **Penelitian ini meneliti pengaruh kualitas program kesadaran keamanan siber, dukungan pimpinan, budaya keamanan siber, dan keterlibatan pegawai terhadap akuntabilitas pegawai pada Bank XYZ. Populasi penelitian terdiri dari 16,500 pegawai. Sampel penelitian sebanyak 170 kuesioner disebar dan 158 kuesioner dikembalikan. Dari respon yang dikembalikan sebanyak 150 respon dianggap valid dan diolah. Penelitian ini adalah penelitian kuantitatif, dengan menggunakan instrumen kuesioner bersifat bersifat skala likert. Sampel terukur diukur dengan Partial Least Square Structural Equation Modelling (PLS-SEM). Hasil analisis menunjukkan bahwa kualitas program kesadaran keamanan siber berpengaruh positif dan signifikan terhadap keterlibatan pegawai (β = 0,195; p = 0,014) dan akuntabilitas pegawai(β = 0,206; p = 0,010). Keterlibatan pegawai berpengaruh positif dan signifikan terhadap akuntabilitas pegawai (β = 0,222; p = 0,008) dan memediasi secara parsial hubungan antara kualitas program dan akuntabilitas(β = 0,043; p = 0,046). Dukungan pimpinan berpengaruh positif dan signifikan terhadap budaya keamanan siber (β = 0,566; p < 0,001). Budaya keamanan siber berpengaruh positif dan signifikan terhadap keterlibatan pegawai (β = 0,265; p = 0,001) namun tidak berpengaruh signifikan terhadap akuntabilitas pegawai (β = 0,092; p = 0,257). Penelitian ini dapat ditarik kesimpulan bahwa kualitas program kesadaran keamanan siber secara langsung dan tidak berpengaruh terhadap akuntabilitas pegawai, secara tidak langsung dan tidak berpengaruh terhadap akuntabilitas pegawai melalui keterlibatan pegawai, serta dukungan pimpinan berpengaruh signifikan terhadap budaya keamanan siber.**
Kata kunci— akuntabilitas, budaya keamanan, dukungan pimpinan, kesadaran keamanan siber, keterlibatan pegawai, PLS-SEM

I. INTRODUCTION

The objective of this study is to examine the relationship between the quality of cybersecurity awareness programme, leadership support, cybersecurity culture and employee engagement with employee accountability at Bank XYZ. The study population comprises 16,500 employees. For the sample, 170 questionnaires were distributed and 158 returned; of which 150 were found valid and included for data processing. This is a quantitative study using Likert Scale questionnaire instrument. The structural relationships were assessed using Partial Least Squares Structural Equation Modelling (PLS-SEM). The analysis revealed that cybersecurity awareness program quality exerted a positive and statistically significant effect on both employee engagement (β = 0.195; p = 0.014) and employee accountability (β = 0.206; p = 0.010). Employee engagement, in turn, was positively and significantly associated with employee accountability (β = 0.222; p = 0.008). The significant indirect effect of program quality on accountability through employee engagement (β = 0.043; p = 0.046) further confirmed the partial mediating role of employee engagement. Regarding the organisational pathway, leadership support was found to positively and significantly influence cybersecurity culture (β = 0.566; p < 0.001). Cybersecurity culture subsequently demonstrated a positive and significant effect on employee engagement (β = 0.265; p = 0.001); however, its direct effect on employee accountability was not statistically significant (β = 0.092; p = 0.257). The study results show that

the quality of the cybersecurity awareness programme influences employee accountability directly and indirectly (through employee engagement), leadership support has a significant effect on the cybersecurity culture.

The banking industry is currently undergoing strong digital transformation. In this process, the increased reliance on information technology to deliver services, perform operational activities, and manage data has enhanced both the opportunities and vulnerabilities for organisations. Digitalisation can bring banking services more efficiency, quicker processing, and wider accessibility to customers. Yet, it also amplifies the risks of various cyber attacks such as phishing, malware, ransomware, credential theft, data leakage and social engineering. Cybersecurity incidents in the banking industry will have considerable financial losses but also affect customer trust, organisational reputation, regulatory compliance, and business continuity. As emphasized in the regulatory provision on cyber resilience and cyber security in commercial banks, which is de facto adopted by the Banking Authority in Indonesia [1]; cybersecurity management is highly valued in ensuring the resilience and continuity of the banking industry.

Despite organisations' increasing investment in security technologies and controls, the human factor continues to be one of the leading causes of risk. Failure to recognise threats, weak passwords, disclosing sensitive information, not reporting suspicious activity, and non-compliance are all factors which may result in a failure of technical controls. These realities demonstrate the fact that cybersecurity is not only technology-dependent but also depends on individual knowledge, perception, engagement, and behaviour. In the absence of security awareness and behaviour, employees may be the first line of defence as well as being a source of vulnerability [2].

To counter user-related risk, organisations deploy cybersecurity awareness programmes using online training, interactive workshops, phishing simulations, communication programmes, newsletters and continuing training activities [3], [4]. These programmes are designed to increase employees' risk awareness, increase secure behaviour and improve compliance with information security policies and procedures. Rarely, however, does programme evaluation progress beyond administrative output such as participant enrollment and completion, attendance and completion of individual training modules, and results of phishing simulation activities. These outcomes are not likely to reflect increased engagement and accountability in employees' discharge of day-to-day security responsibilities [5], [6]. Evaluation of programme success should, therefore, appreciate administrative outputs associated with individual and organisational impact on employee behavioural change.

Prior studies have explored a number of factors that influence the effectiveness of security awareness programs. The effectiveness of Security Education, Training, and Awareness (SETA) programs depends on the quality of content, delivery modes, organisational support, and employee engagement [3]. In addition, other studies emphasize the role of security culture in fostering information security values, norms, and practices, and leadership support in building an environment that promotes better security practices [2], [7], [8]. However, these factors are typically analyzed independently. There is a lack of models that integrate awareness program quality, leadership support, cybersecurity culture, employee engagement, and employees' sense of accountability, particularly in the Indonesian banking sector.

Based on this review, four research gaps are identified. First, the evaluation of cybersecurity awareness programs still emphasises administrative outputs rather than employee behavioural outcomes. Second, employee cybersecurity accountability remains relatively under-examined compared with information security awareness and compliance. Third, employee engagement has rarely been tested as a mechanism explaining the relationship between awareness program quality and accountability. Fourth, integrated models covering program quality, leadership support, cybersecurity culture, engagement and accountability are scarce, particularly in the Indonesian banking industry.

The novelty of this study lies in the development of an evaluation model that separates administrative program outputs from employee behavioural outcomes. The study conceptualises employee accountability as a behavioural outcome that should be considered in measuring awareness program effectiveness and evaluates employee engagement as a mediating mechanism in the program quality-accountability relationship. From an organisational viewpoint, leadership support is conceptualised as an antecedent of cybersecurity culture and cybersecurity culture is linked to employee engagement and accountability.

This study examines an integrated model linking cybersecurity awareness program quality, cybersecurity culture, employee engagement, employee accountability, and leadership support within Bank XYZ. More specifically, it evaluates whether program quality influences engagement and accountability, whether engagement mediates the relationship between program quality and accountability, whether leadership support shapes cybersecurity culture, and whether that culture affects engagement and accountability. Partial Least Squares Structural Equation Modelling (PLS-SEM) is employed to estimate both the direct relationships and the mediated pathway among the constructs. Through this investigation, the study seeks to advance the literature on evaluating cybersecurity awareness program effectiveness while offering practical guidance to organisations seeking to implement such programs with a stronger emphasis on employee engagement and accountability.

II. BACKGROUND AND HYPOTHESIS DEVELOPMENT

A. Theoretical Perspective

Protection Motivation Theory (PMT) serves as the conceptual lens for explaining the formation of protective behavior among employees. According to PMT, motivation to adopt protective actions develops through threat appraisal and coping appraisal. Threat appraisal concerns an individual’s assessment of how likely a threat is to occur and how serious its consequences may be, whereas coping appraisal reflects beliefs about the

e-ISSN: 2828-6707
https://esensijournal.com/index.php/infokom
DOI: 10.55886/infokom.v10i2.538

effectiveness of the available response and one's ability to carry it out successfully. In the information security context, awareness programs can strengthen employees' understanding of cyber threats, their possible consequences, and appropriate mitigation measures. Leadership support and a well-established cybersecurity culture, in turn, can provide the legitimacy, resources, shared norms, and encouragement needed to sustain secure behavior. Accordingly, PMT is applied in this study as an explanatory perspective on the development of protective behavior rather than as a complete theoretical model whose entire set of components is tested directly.

B. Awareness Program Quality and Employee Engagement

Cybersecurity awareness program quality reflects the capability of a program to deliver material that is relevant, current, comprehensible, accessible, interactive, and aligned with job requirements. A high-quality program not only conveys information but also creates a learning experience capable of increasing employee attention and participation. Content quality, delivery method, opportunities for practice, and the fit between material and job characteristics are important determinants of SETA program effectiveness [3]. Relevant and interactive programs also tend to encourage active participation and reduce fatigue towards cybersecurity communication [6]. The following hypothesis is therefore proposed.

H1: Cybersecurity awareness program quality has a positive effect on employee engagement.

C. Employee Engagement and Accountability

Employee engagement describes an individual's attention, participation, and commitment to the organisation's cybersecurity activities. Highly engaged employees tend to participate more actively in training, understand policies, seek relevant information, apply security practices, and report suspicious activity. Employee accountability refers to an individual's awareness of and willingness to take responsibility for security-related actions, including complying with policies, safeguarding information confidentiality, reporting potential incidents, following up on risks, and accepting the consequences of inappropriate actions. Engagement provides employees with the opportunity to understand the risks and consequences of their actions, thereby encouraging more responsible behaviour [10].

H2: Employee engagement has a positive effect on employee accountability.

In addition to enhancing engagement, a high-quality cybersecurity awareness program may directly influence employee accountability. Programs that are relevant and easy to understand help employees comprehend threats, policies, procedures, role allocation, behavioural standards, reporting mechanisms, and the consequences of security-related actions. Such clarity reduces uncertainty about the actions required when employees encounter a potential incident. Previous studies likewise indicate that the quality of training and awareness programs is associated with information security behaviour and compliance with organisational policies [3], [5].

H3: Cybersecurity awareness program quality has a positive effect on employee accountability.

The effect of program quality on accountability may also operate through employee engagement. A high-quality program can attract attention, encourage participation, and strengthen commitment to cybersecurity. The resulting engagement helps employees internalise the program material and connect it to their day-to-day security responsibilities. Within this mechanism, program quality provides supportive learning conditions, while engagement helps convert the learning experience into responsible behaviour.

H4: Employee engagement mediates the effect of cybersecurity awareness program quality on employee accountability.

D. Leadership Support and Cybersecurity Culture

Beyond program quality, the effectiveness of cybersecurity management is influenced by organisational factors. Leadership support represents management commitment expressed through communication, provision of resources, priority setting, supervision, allocation of time for program participation, and behavioural role modelling. Such support signals that cybersecurity is an organisational priority and part of every individual's responsibility. Leaders also shape cybersecurity culture, because their decisions and behaviour influence priorities, resource allocation, and employees' perceptions of the importance of security. Consistent leadership support can create an environment that encourages open communication, compliance, and the application of cybersecurity practices [8].

H5: Leadership support has a positive effect on cybersecurity culture.

Cybersecurity culture describes the shared values, norms, beliefs, and practices that support security behaviour within an organisation [7]. When cybersecurity becomes a shared value and norm, employees obtain social and organisational reinforcement to attend training, pay attention to security communication, discuss risks, and report suspicious activity. A positive culture also helps employees regard cybersecurity as part of their work rather than as an additional obligation separate from their primary responsibilities. Shared norms, open communication, and support for learning can increase employees' willingness to participate in cybersecurity activities [2], [7].

H6: Cybersecurity culture has a positive effect on employee engagement.

A positive cybersecurity culture also provides values and norms that help employees understand expected behaviour. In such an environment, compliance, incident reporting, data protection, and risk follow-up are regarded as shared responsibilities. Cybersecurity culture may strengthen behavioural consistency because security actions are grounded not only in written rules but also in habits and social expectations in the workplace. Employees working within a positive cybersecurity culture are expected to be better able to understand and discharge security responsibilities consistently [2].

H7: Cybersecurity culture has a positive effect on employee accountability.

The conceptual framework of the study, comprising the five constructs and the seven hypothesised relationships, is presented in Figure 1.

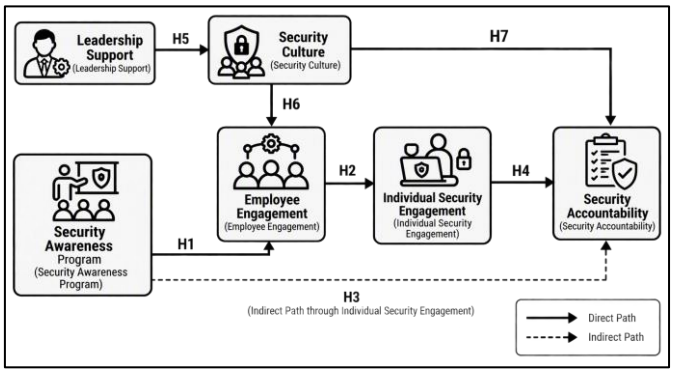


Figure 1. Research conceptual framework

III. RESEARCH METHODOLOGY

A. Design, Population, and Sample

An explanatory quantitative study was conducted using a cross-sectional survey to investigate the relationships among cybersecurity awareness program quality, leadership support, cybersecurity culture, employee engagement, and employee accountability. All constructs were examined using observations obtained within the same data-collection period.

The target population comprised 16,500 employees of Bank XYZ. Eligibility was restricted to active employees who had previously participated in cybersecurity awareness activities organised by the institution, thereby ensuring that respondents had relevant experience from which to assess the constructs under study. Participants were selected purposively on the basis of these criteria, and responses were obtained through an online questionnaire administered between January and February 2026.

Questionnaire invitations were sent to 170 employees who met the eligibility requirements. A total of 158 completed questionnaires were returned, corresponding to a response rate of 92.9%. The responses were subsequently screened for completeness, consistency, and compliance with the data-eligibility requirements. Eight submissions were removed during this process, leaving 150 usable responses for the analysis.

Application of the Cochran formula [11], using a 95% confidence level and a 5% margin of error, indicated that 376 respondents would be required to support full statistical generalisation to the employee population. The final analytical sample of 150 was therefore below this benchmark. Nevertheless, the sample was treated as meeting the minimum analytical requirement adopted for PLS-SEM in this study [12]. PLS-SEM was employed because the proposed model involves several latent constructs and requires the estimation of both direct and indirect relationships, with an emphasis on model development and prediction. Accordingly, the findings are interpreted as empirical evidence of the relationships observed among the analysed respondents, rather than as results that can be generalised without qualification to all 16,500 employees of Bank XYZ.

Participation was voluntary. All data were collected anonymously and used solely for research purposes. Respondent identities were neither recorded nor published, so that confidentiality and privacy were maintained. A summary of questionnaire distribution is presented in Table I.

TABLE I
DISTRIBUTION OF RESEARCH QUESTIONNAIRES

Description	Number	Percentage
Questionnaires distributed	170	100.0%
Questionnaires returned	158	92.9%
Incomplete / ineligible	8	4.7%
Responses analysed	150	88.2%

Note: percentages are calculated against the number of questionnaires distributed.

B. Instrument and Data

Research data were obtained through a questionnaire distributed to employees of Bank XYZ who met the sampling criteria. The questionnaire employed a five-point Likert response format anchored at 1 (strongly disagree) and 5 (strongly agree). This format provided a structured means of capturing respondents' perceptions of the study constructs while remaining straightforward to understand and use.

The study employs five main constructs: awareness program quality, leadership support, cybersecurity culture, employee engagement, and employee accountability. Each construct is measured using four reflective indicators developed from concepts and findings of previous research in cybersecurity awareness, security culture, and employee engagement. All indicators were adapted to the banking industry context and the objectives of the study.

Awareness program quality is defined as employees' perceptions of the relevance, currency, interactivity, accessibility, and effectiveness of the organisation's cybersecurity awareness program. Leadership support reflects employees' perceptions of management commitment to supporting cybersecurity implementation. Cybersecurity culture represents the organisational values, norms, and practices that encourage information security behaviour. Employee engagement indicates the level of attention, participation, and commitment of employees towards cybersecurity activities. Employee accountability reflects the degree of individual responsibility in applying and complying with the organisation's cybersecurity principles. The constructs, codes, operational definitions, and number of indicators are summarised in Table II.

TABLE II
CONSTRUCTS, OPERATIONAL DEFINITIONS, AND INDICATORS

Construct	Code	Operational Definition (4 items each)
Awareness program quality	KP	Perception of awareness program quality
Leadership support	DP	Perception of leadership support
Cybersecurity culture	BK	Perception of cybersecurity culture
Employee engagement	KT	Level of employee engagement
Employee accountability	AK	Level of employee accountability

C. Data Analysis

The empirical data were examined through Partial Least Squares Structural Equation Modeling (PLS-SEM) in order to evaluate the hypothesized relationships that link awareness program quality, leadership support, cybersecurity culture, employee engagement, and employee accountability. The analytical procedure was organized into three sequential phases, namely descriptive statistical examination, assessment of the measurement model, and evaluation of the structural model.

Descriptive statistics were generated to characterize the profile of the respondents and to summarize the distribution of responses across every indicator. Following this preliminary stage, the measurement model was scrutinized in order to establish the psychometric quality of each latent construct. Convergent validity was appraised by inspecting the outer loadings together with the Average Variance Extracted (AVE). An indicator was regarded as acceptable when its outer loading reached or exceeded 0.70, whereas each construct was expected to record an AVE of at least 0.50. Internal consistency reliability was subsequently verified through Composite Reliability (CR), and values equal to or greater than 0.70 were interpreted as evidence of adequate reliability [12].

Evaluation of the structural model was then carried out in order to test the postulated relationships among the constructs, with analytical attention directed to the path coefficients (β), the corresponding t-statistics, and the associated p-values. The coefficient of determination (R^2) was employed to quantify the proportion of variance in the endogenous constructs that could be explained by the exogenous constructs. In addition, the effect size (f^2) was computed to gauge the incremental contribution of each exogenous construct within the specified model, while the predictive relevance (Q^2) was examined to appraise the predictive capability of the model [12].

Hypothesis testing was performed by means of the bootstrapping procedure that is embedded within PLS-SEM, which produces empirical resampling distributions for the estimated parameters. A hypothesized relationship was regarded as statistically significant whenever its p-value satisfied the predetermined threshold of $p < 0.05$, and the direction of the relationship was inferred from both the sign and the magnitude of the corresponding path coefficient. All analyses reported in the present study were conducted using the empirical data obtained from the 150 eligible responses that had successfully passed the earlier screening criteria.

IV. RESULTS AND DISCUSSION

A. Respondent Characteristics

Of the 150 respondents analysed, 83 (55.3%) were female and 67 (44.7%) were male. By age group, the majority were aged 18–25 years (71 respondents, 47.3%), followed by 26–35 years (48 respondents, 32.0%), 36–45 years (22 respondents, 14.7%), and above 45 years (9 respondents, 6.0%).

In terms of education, most respondents held a bachelor's degree (72 respondents, 48.0%). Respondents with senior high school education or equivalent numbered 46 (30.7%), those with a diploma 18 (12.0%), and those with a master's degree 14 (9.3%).

These characteristics indicate that the study is dominated by employees of productive age with secondary to higher educational backgrounds. The diverse composition of respondents is expected to provide an informative picture of employee perceptions of the cybersecurity awareness program, leadership support, cybersecurity culture, engagement, and accountability within a banking organisation. A summary of respondent characteristics is presented in Table III.

TABLE III
DEMOGRAPHIC CHARACTERISTICS OF RESPONDENTS

Characteristic	Category	n	%
Gender	Male	67	44.7
	Female	83	55.3
Age	18–25 years	71	47.3
	26–35 years	48	32.0
	36–45 years	22	14.7
	> 45 years	9	6.0
Education	Senior high school	46	30.7
	Diploma	18	12.0
	Bachelor's degree	72	48.0
	Master's degree	14	9.3

B. Descriptive Statistics

Based on the analysis of 150 responses, construct means ranged from 3.877 to 3.988 on the five-point Likert scale. Employee engagement (KT) recorded the highest mean of 3.988 with a standard deviation of 0.492, while awareness program quality (KP) and cybersecurity culture (BK) shared the same mean of 3.877. Employee accountability (AK) recorded a mean of 3.902 and leadership support (DP) a mean of 3.880.

All constructs recorded means above the midpoint of the measurement scale, indicating that respondents held relatively positive perceptions of the variables examined. Standard deviations ranging from 0.492 to 0.558 indicate moderate variation in responses without any extreme dispersion of data.

These findings provide an initial indication that respondents generally hold a favourable perception of the implementation of the cybersecurity awareness program and related

organisational factors. Descriptive analysis alone, however, cannot explain causal relationships among constructs; further testing through measurement and structural model evaluation using PLS-SEM is therefore required. The descriptive statistics are summarised in Table IV.

TABLE IV
DESCRIPTIVE STATISTICS OF RESEARCH CONSTRUCTS

Construct	Code	Mean	SD
Awareness program quality	KP	3.877	0.511
Leadership support	DP	3.880	0.558
Cybersecurity culture	BK	3.877	0.529
Employee engagement	KT	3.988	0.492
Employee accountability	AK	3.902	0.525

C. Measurement Model

The results of convergent validity and construct reliability evaluation are presented in Table V.

TABLE V
CONVERGENT VALIDITY AND CONSTRUCT RELIABILITY

Construct	Indicator	Outer Loading	AVE	CR
Awareness program quality	KP1	0.812	0.668	0.889
	KP2	0.834		
	KP3	0.791		
	KP4	0.834		
Leadership support	DP1	0.821	0.674	0.892
	DP2	0.847		
	DP3	0.801		
	DP4	0.814		
Cybersecurity culture	BK1	0.846	0.704	0.905
	BK2	0.862		
	BK3	0.817		
	BK4	0.831		
Employee engagement	KT1	0.828	0.682	0.895
	KT2	0.851		
	KT3	0.806		
	KT4	0.823		
Employee accountability	AK1	0.819	0.677	0.893
	AK2	0.842		
	AK3	0.804		
	AK4	0.827		

Assessment of the measurement model confirmed that every indicator recorded an outer loading exceeding 0.70. The Average Variance Extracted (AVE) values obtained across all constructs fell within the interval of 0.668 to 0.704, demonstrating that each construct accounted for more than 50% of the variance observed in its associated indicators. In parallel, the Composite Reliability (CR) coefficients ranged from 0.889 to 0.905, providing evidence of excellent internal consistency across all latent variables. Taken together, these findings establish that every construct fulfilled the required thresholds for both convergent validity and construct reliability, thereby qualifying the measurement model for subsequent structural model evaluation.

D. Structural Model

The results of hypothesis testing using the bootstrapping procedure in PLS-SEM are presented in Table VI.

TABLE VI
HYPOTHESIS TESTING AND STRUCTURAL MODEL RESULTS

Hypothesis	Path	β	t	p	Decision
H1	KP → KT	0.195	2.486	0.014	Supported
H2	KT → AK	0.222	2.712	0.008	Supported
H3	KP → AK	0.206	2.597	0.010	Supported
H4	KP → KT → AK	0.043	2.010	0.046	Supported (partial mediation)
H5	DP → BK	0.566	8.362	< 0.001	Supported
H6	BK → KT	0.265	3.374	0.001	Supported
H7	BK → AK	0.092	1.139	0.257	Not supported

Six of the seven proposed hypotheses were supported. The quality of cybersecurity awareness programs significantly enhanced both employee engagement ($\beta = 0.195$, $p = 0.014$) and employee accountability ($\beta = 0.206$, $p = 0.010$). Employee engagement was also found to positively influence employee accountability ($\beta = 0.222$, $p = 0.008$). Furthermore, leadership support emerged as a strong predictor of cybersecurity culture ($\beta = 0.566$, $p < 0.001$), while cybersecurity culture significantly increased employee engagement ($\beta = 0.265$, $p = 0.001$). However, the direct relationship between cybersecurity culture and employee accountability was not statistically significant ($\beta = 0.092$, $p = 0.257$), suggesting that the influence of cybersecurity culture on accountability may occur indirectly through other organizational factors.

The structural model evaluation yielded R^2 values of 0.321 for cybersecurity culture, 0.099 for employee engagement, and 0.123 for employee accountability, indicating that the model explains 32.1%, 9.9%, and 12.3% of the variance in these endogenous constructs, respectively. The R^2 value for cybersecurity culture indicates a stronger explanatory capability than that for the other constructs, whereas the R^2 values for employee engagement and accountability indicate that additional factors outside the research model also influence these two constructs.

e-ISSN: 2828-6707
https://esensijournal.com/index.php/infokom
DOI: 10.55886/infokom.v10i2.538

The mediation effect was tested by evaluating the indirect effect using the bootstrapping procedure in PLS-SEM. The mediating effect of awareness program quality on employee accountability through employee engagement was evaluated on the basis of the indirect effect coefficient, the t-statistic, and the p-value. Using this approach, the significance of the indirect effect is determined empirically from the bootstrapping results rather than solely from the manual multiplication of path coefficients.

E. Discussion

The results show that cybersecurity awareness program quality has a positive and significant effect on employee engagement. Programs offering relevant, current, and accessible material, together with opportunities for practice, encourage employee engagement in the cybersecurity learning process. Employee engagement, in turn, has a positive and significant effect on accountability. Employees who are more engaged in awareness activities tend to have a better understanding of security risks and responsibilities, including recognising suspicious activity, reporting potential incidents, and following up on corrective actions. This finding is consistent with PMT, which explains that individuals tend to display protective behaviour when they understand the threats they face and believe in the effectiveness of the available preventive measures [9]. Relevant and comprehensible awareness programs can increase employees' motivation to engage in cybersecurity activities and thereby support the formation of safer behaviour.

Beyond its indirect effect through engagement, awareness program quality also exerts a positive and significant direct effect on employee accountability. This indicates that the relationship between program quality and accountability does not depend entirely on employee engagement, and that the quality of program design and delivery may contribute to accountability through more than one mechanism. The results further show that employee engagement partially mediates the relationship between awareness program quality and accountability, indicating that high-quality programs enhance accountability not only directly but also by increasing employee participation and engagement in cybersecurity activities.

Leadership support demonstrates a positive and significant effect on cybersecurity culture and represents the predictor with the largest path coefficient in the model. This finding indicates that the legitimacy provided by leaders, consistency of security messaging, support for time allocation, and leadership role modelling all contribute to shaping the cybersecurity culture environment of the organisation [8]. Cybersecurity culture, in turn, has a positive and significant effect on employee engagement. The direct effect of cybersecurity culture on employee accountability is not significant once the other variables in the model are accounted for, suggesting that cybersecurity culture does not directly explain variation in accountability within this model and that its influence on accountability may operate through employee engagement or other organisational mechanisms.

The non-significant direct relationship between cybersecurity culture and employee accountability indicates that the presence of a positive security culture does not automatically translate into responsible behaviour at the individual level [2], [7]. Accountability may be more strongly influenced by personal factors such as risk understanding, experience, procedural compliance, and organisational supervision. This finding suggests that cybersecurity culture functions primarily as a contextual factor that encourages employee engagement rather than as a direct determinant of accountability.

Theoretically, the results support PMT in the context of organisational cybersecurity. Awareness program quality and organisational factors contribute to the formation of employee engagement, which subsequently influences cybersecurity accountability. The study also demonstrates that employee engagement serves as an important mechanism bridging awareness program quality and employee accountability.

Practically, the findings carry implications for the management of cybersecurity awareness programs at Bank XYZ. Program evaluation should extend beyond administrative outputs such as participant numbers and training completion rates to encompass outcomes relating to the quality of the learning experience, employee engagement, phishing simulation results, reporting behaviour, leadership support, cybersecurity culture, and the follow-up of security findings. Awareness measurement dashboards can therefore be developed to distinguish program output indicators from behavioural and organisational outcome indicators. This approach can help organisations obtain a more comprehensive picture of program effectiveness and identify areas requiring improvement.

V. CONCLUSION

The results of this study indicate that effective cybersecurity awareness programs play a critical role in strengthening employee engagement and accountability. Among all examined relationships, leadership support emerged as the most influential factor, significantly shaping cybersecurity culture within the organization. While a strong cybersecurity culture was associated with higher levels of employee engagement, it did not directly translate into greater accountability once other determinants were included in the model. The partial mediating role of employee engagement further highlights that awareness initiatives are most effective when they actively encourage employee participation and involvement. Therefore, organizations seeking to improve cybersecurity accountability should focus not only on enhancing awareness program quality but also on fostering employee engagement and securing strong leadership commitment.

This study is subject to several limitations that provide opportunities for future research. The relatively small sample size, compared with the number suggested by Cochran's formula, may constrain the external validity of the findings. Furthermore, the purposive sampling approach raises concerns regarding sample representativeness and potential selection bias. The cross-sectional design also limits the ability to capture

temporal changes in cybersecurity behaviour and prevents stronger conclusions regarding causality.

Future studies should seek to overcome these limitations by adopting larger and more representative samples, as well as longitudinal designs that allow researchers to examine how cybersecurity awareness, engagement, and accountability develop over time. Moreover, expanding the model to include variables such as information security compliance, risk perception, incident experience, and organisational control mechanisms may provide a more comprehensive explanation of cybersecurity accountability. The integration of objective behavioural measures, including phishing test outcomes, training participation records, and incident reporting statistics, would further enhance the reliability and practical relevance of future research findings.

Overall, the study provides empirical evidence on the relationships among cybersecurity awareness program quality, leadership support, cybersecurity culture, employee engagement, and employee accountability at Bank XYZ. The effectiveness of cybersecurity awareness programs is determined not only by the delivery of training but also by employee engagement, leadership support, and the cybersecurity culture developed within the organisation. Evaluation of awareness programs therefore needs to be developed more comprehensively by distinguishing program outputs, such as training completion rates, from outcomes reflecting changes in employees' cybersecurity behaviour, thereby helping organisations measure program effectiveness more holistically and identify the areas requiring improvement to strengthen employees' security behaviour and accountability.

ACKNOWLEDGMENTS

The author gratefully acknowledges the management and employees of Bank XYZ for their time, cooperation, and valuable contributions during the data collection phase of this study. Appreciation is also extended to Universitas Satya Negara Indonesia for the academic guidance, resources, and institutional support provided throughout the research process.

REFERENCES

[1] T. O. Abrahams, O. A. Farayola, S. Kaggwa, P. U. Uwaoma, A. O. Hassan, and S. O. Dawodu, "Cybersecurity awareness and education programs: A review of employee engagement and accountability," *Computer Science & IT Research Journal*, vol. 5, no. 1, pp. 100–119, 2024, doi: 10.51594/csitrj.v5i1.708.

[2] M. Alshaikh, "Developing cybersecurity culture to influence employee behavior: A practice perspective," *Computers & Security*, vol. 98, Art. no. 102003, 2020.

[3] A. Alyami, D. Sammon, K. Neville, and C. Mahony, "The critical success factors for Security Education, Training and Awareness program effectiveness: A lifecycle model," *Information Technology & People*, vol. 36, no. 8, pp. 94–125, 2023.

[4] S. Chaudhary, V. Gkioulos, and S. Katsikas, "Developing metrics to assess the effectiveness of cybersecurity awareness program," *Journal of Cybersecurity*, vol. 8, no. 1, Art. no. tyac006, 2022.

[5] W. G. Cochran, *Sampling Techniques*, 3rd ed. New York, NY, USA: John Wiley & Sons, 1977.

[6] R. Fisher, C. Porod, and S. Peterson, "Motivating employees and organizations to adopt a cybersecurity-focused culture," *Journal of Organizational Psychology*, vol. 21, no. 1, pp. 114–131, 2021.

[7] J. F. Hair, J. J. Risher, M. Sarstedt, and C. M. Ringle, "When to use and how to report the results of PLS-SEM," *European Business Review*, vol. 31, no. 1, pp. 2–24, 2019.

[8] Otoritas Jasa Keuangan, *Surat Edaran Otoritas Jasa Keuangan Republik Indonesia Nomor 29/SEOJK.03/2022 tentang Ketahanan dan Keamanan Siber bagi Bank Umum*, 2022.

[9] A. Reeves, P. Delfabbro, and D. Calic, "Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue," *SAGE Open*, vol. 11, no. 1, 2021.

[10] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change," *The Journal of Psychology*, vol. 91, no. 1, pp. 93–114, 1975.

[11] B. Uchendu, J. R. C. Nurse, M. Bada, and S. Furnell, "Developing a cyber security culture: Current practices and future needs," *Computers & Security*, vol. 109, Art. no. 102387, 2021.

[12] W. Yeoh, H. Huang, W. S. Lee, F. Al Jafari, and R. Mansson, "Simulated phishing attack and embedded training campaign," *Journal of Computer Information Systems*, vol. 62, no. 4, pp. 802–821, 2022.