INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 13, Issue 8, (2023) E-ISSN: 2222-6990

Enhancing Cybersecurity Awareness among Banking Employees in Malaysia: Strategies, Implications, and Research Insights

Santhananthan Gopal Krishnan, Abdulaziz Al-Nahari, Noor Azma Ismail* & Danny Ngo Lung Yao

School of Information Technology, UNITAR International university, Petaling Jaya, Selangor, Malaysia

Email: gksanthana@yahoo.com, abdulaziz.yahya@unitar.my, azma1706@unitar.my, danny.ngo@unitar.my

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v13-i8/17413 DOI:10.6007/IJARBSS/v13-i8/17413

Published Date: *15* August 2023

Abstract

Cybersecurity awareness is important for employees in Malaysia's banking sector. Protecting valuable data from theft and misuse requires fostering a culture of awareness and providing comprehensive security training. Unintentional disclosure of sensitive information poses a significant risk, leading to cyberattacks and loss of clients, eventually impacting profitability. This paper explores the dependent variable of cybersecurity awareness and delves into independent variable analysis, strategies, and the existing lack of cyber security measures. A sample of 384 employees from a Malaysian banking organization was selected using the Krejcie & Morgan sampling technique. Data analysis was conducted and demonstrating good internal consistency and mitigating concerns about measurement reliability. Furthermore, collinearity issues were absent, as indicated by VIF values below ten and tolerance values exceeding 0.1 for the examined independent variables.

Keywords: Banking Sector, Cybersecurity, Awareness, Krejcie & Morgan Sampling Techniques

Introduction

In the competitive market of Malaysia's banking sector, the imperative of enhancing cybersecurity awareness among employees cannot be overstated. Insufficient awareness in this domain exposes banking enterprises to multifaceted risks, including the unauthorized acquisition and exploitation of invaluable data, inadvertent information disclosure, and the proliferation of sophisticated cyber threats. These challenges, when left unaddressed, culminate in the erosion of customer trust, a substantial decline in organizational profitability, and the erosion of the institution's hard-earned reputation. However, the implementation of a comprehensive and well-crafted cybersecurity training program holds the potential to serve as an effective panacea to these pressing concerns. By equipping employees with the requisite competencies and knowledge to safeguard critical data and navigate evolving

threats, Malaysian banks can fortify their defensive posture and proactively preserve the sanctity of customer interests. Furthermore, scholarly research underscores the significance of robust information security governance, the imposition of stringent limitations on cyber operations, and the establishment of a secure operational environment. By embracing a proactive stance towards cybersecurity awareness and training initiatives, Malaysian banking institutions can fortify their defenses, proactively safeguard customer interests, and bolster their overall resilience amidst the relentless onslaught of ever-evolving cyber adversaries. Therefore, the aim of this article is to determine the advantages of cyber security awareness among bank employees, identify risks arising from a lack of awareness, and formulate strategies to mitigate these issues. By identifying the risks associated with a lack of awareness and formulating strategies to address these issues, this study highlights the importance of this topic. Furthermore, it emphasizes the utility and effectiveness of cybersecurity training, specifically tailored to the banking industry.

The significance of this study lies in its potential to equip banking institutions with the necessary tools and knowledge to fortify their defensive posture. By instilling the requisite competencies among employees, banks can ensure the protection of critical data and navigate the evolving cyber landscape with confidence. Additionally, this research contributes valuable insights into the establishment of robust information security governance, the imposition of stringent limitations on cyber operations, and the creation of a secure operational environment.

By adopting a proactive stance towards cybersecurity awareness and training initiatives, Malaysian banking institutions can bolster their overall resilience in the face of ever-evolving cyber threats. This article serves as a guide, offering research insights and practical strategies for banks to strengthen their defences. Ultimately, it is through prioritizing cybersecurity awareness and implementing effective measures that the banking sector can preserve customer trust, protect its reputation, and ensure long-term success in the dynamic landscape of the digital age.

Literature Review

Security awareness encapsulates individuals' attitudes and knowledge pertaining to specific organizations (Dharmawansa and Madhuwanthi, 2020). Complementarily, Williams, et al (2019) highlight the tangible benefits of providing security awareness training and fortifying banking and financial institutions against an array of cyber threats. Security awareness matters in mitigating substantial financial losses and preserving reputational integrity amidst the pervasive data breaches experienced by banks and financial entities (Al-Shanfari et al., 2020). As the digital reliance on online banking burgeons, heightened user vigilance when accessing banking websites becomes imperative (Jaeger and Eckhardt, 2021). Salleh and Janczewski (2019) caution against conducting online banking operations on publicly shared computers or devices, emphasizing the criticality of upholding robust cyber security measures to protect debit and credit card information.

The expertise required for banking personnel to navigate the intricacies of information system security is paramount. Beyond relying on usernames and passwords, effective information security encompasses data confidentiality, integrity, and availability. Cultivating a robust security culture, promoting awareness of vulnerabilities and threats, and driving behavioral changes are essential. Emphasizing Information Security Awareness (ISA), including comprehension and adherence to security practices, is crucial (Dharmawnsa and

Madhuwanthi, 2020). Encrypted apps serve as indispensable remote security tools for secure communication and encryption of financial correspondence (Dharmawnsa and Madhuwanthi, 2020). Treating company information security as a critical concern, combining technological measures with personnel responsibilities, and setting an example for employees is vital. Ongoing support is necessary to implement effective security measures, particularly for organizations managing significant amounts of personal data. Security Education, Training, and Awareness (SETA) play a central role in managing evolving information security risks, as highlighted in the implementation of Big Data Solutions (BDS) within the banking industry.

Promoting cybersecurity awareness among banks and their users requires the implementation of various effective strategies. These include using only "company-approved work devices" to ensure employees adhere to established policies, which strengthens cybersecurity (Dharmawansa and Madhuwanthi, 2020). Additionally, providing training on phishing scams equips bank employees with the knowledge to prevent fraud and scams, even without extensive IT expertise (Allen et al., 2018). Avoiding the use of personal mobile phones for office work and instead adopting encrypted apps as remote security tools can significantly enhance cybersecurity measures (Dharmawansa and Madhuwanthi, 2020). By implementing these strategies, banks can elevate security awareness, mitigate risks, and protect sensitive information, as supported by research conducted by experts in the field.

Data theft poses multifaceted risks to banks, encompassing operational, strategic, and legal dimensions. To mitigate these risks, a comprehensive approach to risk management is crucial, with emphasis on system architecture, money laundering prevention, and cybersecurity. Strategic missteps can result in security breaches and reputational damage, underscoring the importance of maintaining performance and market reputation. Human factors, including inadequate resources and negligence, contribute to challenges such as human errors, phishing attacks, and compromised credentials, which can have severe consequences for data security and business operations. Effective Occupational Health and Safety (OHS) management is essential for reducing accidents and losses. As banks increasingly rely on Internet technologies and mobile banking, the global cyber threat landscape expands, necessitating collaboration among diverse stakeholders to strengthen cybersecurity defences.

Methodology

Population, Sampling & Measurements

This study distributed questionnaires electronically to bank employees in Malaysia. The respondents are bank employees aged 18 to 60 years old in Malaysia. According to a report by ceicdata.com (2017), the total number of bank employees in Malaysia was 118,851 thousand in 2017. Additionally, Karim et al (2020) stated that the overall working population in Malaysia was 14.96 million (Tjiptono et al., 2020). The sample size was determined based on the guidance of Krejcie & Morgan sampling technique, with a margin of error of 5%. Hence, it is concluded that 384 participants are necessary for a meaningful response to this research survey.

Data was collected using a survey questionnaire that solicited demographic information and measured cybersecurity awareness (the dependent variable) and independent variables such as analysis, strategies, and lack of cybersecurity. A four-point Likert scale was employed to gauge respondents' viewpoints.

Reliability Analysis

Table 1 displays the reliability analysis for each variable in the study, comprising five items. The dependent variable, Cyber Security Awareness, shows a Cronbach's Alpha of 0.812, indicating good internal consistency. Among the independent variables, Strategies exhibit a Cronbach's Alpha of 0.827, signifying good internal consistency, while the variable, Lack of Cyber Security, demonstrates a Cronbach's Alpha of 0.777, representing acceptable internal consistency. Analyse has a Cronbach's Alpha of 0.763, indicating acceptable internal consistency.

Table 1
Reliability Analysis (N =384)

Variables	Cronbach's Alpha	No. of Items	Internal Consistency
Cybersecurity Awareness	0.812	5	Good
Analyse	0.763	5	Acceptable
Strategies	0.827	5	Good
Lack of Cybersecurity	0.777	5	Acceptable

Table 2 presents the reliability statistics for all items in the survey, amalgamating the dependent and independent variables. The Cronbach's Alpha based on Standardized Items stands at 0.937, indicating excellent internal consistency across the 20 items in the questionnaire. This score implies that the survey is highly reliable, with each item consistently gauging the constructs it intends to assess, per the guidelines provided by Hair et al. (2003).

Table 2
Reliability Statistics for all Items.

All Variables	Cronbach's Alpha Based on Standardized Items	No. of Items	Internal Consistency
0.937	0.937	20	Excellent

Mean and Standard Deviation Analysis

Descriptive Statistics display the mean, standard deviation (SD), skewness and kurtosis values of this research. Table 3 presents the descriptive statistics of the responses from the 384 respondents for various statements about cybersecurity in the banking sector.

Table 3
Descriptive Statistics (N=384)

Factors	Mean	SD	Skew	Kurtosis	Min	Max
Do you think awareness about cyber security is important to measure risk for bank employees?	3.6406	.63494	-1.740	2.492	1.00	4.00
Do you agree risk management in digital practice is important to control the Cyber security features in the banking sector?	3.4844	.70786	-1.143	.421	1.00	4.00

What is your opinion on strategic development to control the ethical cyber security in the banking sector?	3.4974	.70061	-1.181	.547	1.00	4.00
Do you think lack of facilities in cyber security has developed risk in the banking sector?	3.4271	.68165	-.927	.265	1.00	4.00
Do you believe promotion of cyber security practice is important to develop awareness about security?	3.4479	.60666	-.610	-.559	2.00	4.00
Do you think data manipulation is a big risk for the banking sector?	3.4688	.70734	-.957	-.409	2.00	4.00
Do you agree that the development of risk has declined the brand value of banks?	3.4167	.66099	-.699	-.573	2.00	4.00
Do you believe that risk has reduced the trust factor for consumers?	3.5052	.64632	-.953	-.196	2.00	4.00
Do you think development of digital facilities at baking has increased the risk factor?	3.4870	.61728	-.787	-.372	2.00	4.00
What is your opinion on awareness development to highlight risk management?	3.3854	.64017	-.555	-.637	2.00	4.00
Do you think promotion strategy is important to control the cyber security risks?	3.4818	.61290	-.751	-.413	2.00	4.00
Do you agree the awareness development is a key strategy to maintain risks?	3.4141	.63650	-.621	-.581	2.00	4.00
Do you agree the training and skill development is important to empower employees against cyber security risk?	3.6328	.58534	-1.589	2.658	1.00	4.00
What is your opinion on ethical control to reduce the cyber security issues in banking?	3.4115	.64834	-.650	-.584	2.00	4.00
Do you believe integration of personal device is a key strategy to mitigate the cyber security issues?	3.4323	.70106	-.831	-.561	2.00	4.00
Do you think issues in cyber security has declined the performance level for banks?	3.4219	0.59074	-.458	-.675	2.00	4.00
Do you agree that lack in cyber security has restricted the banks to provide digital services?	3.3411	0.64292	-.694	.564	1.00	4.00
Do you believe lack of awareness is a key issue in cyber security?	3.2396	0.73687	-.412	-1.069	2.00	4.00

Do you think lack of facilities in cyber security has declined the reputation of banks?	3.5703	0.55998	-.863	-.282	2.00	4.00
Do you think the case of money laundering has increased due to inefficient facility in cybersecurity?	3.4688	0.60809	-.685	-.486	2.00	4.00

The respondents acknowledge the importance of cyber security awareness for measuring risk in the banking sector. This is suggested by the highest mean score of 3.6406 (on a scale of 1 to 4) among all factors considered. This score indicates that most respondents agree or strongly agree that cyber security awareness is crucial for risk measurement among bank employees. The low standard deviation (SD = 0.63494) further underpins this consensus among respondents.

Data also suggests the respondents consider training and skill development vital in empowering employees against a cyber security risk, as indicated by the second-highest mean score of 3.6328. A common theme across all factors is the overall skewness and kurtosis of the responses. Most of the skewness values are negative, suggesting respondents agree or strongly agree with the presented statements. Kurtosis values indicate the absence of extreme outliers in most responses.

The respondents appear to be least convinced about the statement "Lack of awareness is a key issue in cyber security," given its lowest mean score of 3.2396. However, the mean is still above the scale's midpoint (2.5), suggesting a general agreement among respondents, albeit with less intensity than other statements.

The findings suggest a strong consensus among respondents regarding the importance of cyber security awareness, strategic development, and training in mitigating risks in the banking sector. The responses also indicate that there is recognition of the consequences of inadequate cybersecurity, such as the potential decline in the bank's reputation, trust factor for consumers, and brand value. Therefore, the banking industry need to emphasize and promote cybersecurity awareness and practices to manage these risks effectively.

Findings

Table 4 shows that the age range of 41-50 was the most represented among respondents, constituting 29.2%. The 31-40 and 51-60 age categories comprised 20% of the respondents. Furthermore, 18.8% of respondents were aged 26-30, and 11.2% were between 18-25. The gender distribution among respondents was nearly balanced, with females accounting for 49.2% and males making up 50.8%.

Demographic Profile

Table 4

Demographic Profile of Respondents (N =384)

Demographics	**Frequency**	**Percentage (%)**
Gender		
Male	189	49.2
Female	195	50.8
Age		
18-25	43	11.2

26-30	72	18.8
31-40	78	20.3
41-50	112	29.2
51-60	79	20.6
Highest Level of Education		
Secondary school	39	10.2
Diploma	72	18.8
Bachelor's degree	153	39.8
Master's degree	114	29.7
Doctorate degree	6	1.6
Job Title		
Intern / Fresh Graduate	46	12.0
Associate / Executive Level	69	18.0
Manager	147	38.3
Senior Manager	80	20.8
Director / VP / Senior VP	39	10.2
C Level (CIO, CTO, COO, C)	3	0.8
Bank		
Affin Bank	15	3.9
Agro Bank	6	1.6
Al Rajhi Bank	9	2.3
Alliance Bank	12	3.1
AmBank	26	6.8
Bank Negara	22	5.7
Bank Rakyat	3	0.8
Bank Simpanan Nasional	13	3.4
CIMB Bank	60	15.6
Hong Leong Bank	23	6.0
Maybank	58	15.1
Muamalat Bank	12	3.1
OCBC Bank	12	3.1
Public Bank	33	8.6
RHB Bank	33	8.6
Standard Chartered Bank	23	6.0
United Overseas Bank (UOB)	21	5.5

Regarding job titles, 38.1% of respondents occupy managerial roles, with 20.8% in senior management positions. 18% of respondents hold associate or executive-level positions, while 12% are interns or fresh graduates. Additionally, 10.2% of respondents are at the Director/VP/Senior VP or equivalent level, and three are C-level employees.

The final demographic query asked the respondents to identify the bank they are currently working for. CIMB Bank and Maybank emerged as the top two employers, with 15.6% and 15.1% of respondents, respectively. Public Bank and RHB Bank followed, each with 8.6% of respondents. Other banks where respondents are employed include Affin Bank, Agro Bank,

Al Rajhi Bank, Alliance Bank, AmBank, Bank Negara, Bank Rakyat, Bank Simpanan Nasional, Hong Leong Bank, OCBC Bank, Standard Chartered Bank, and United Overseas Bank (UOB).

Correlation Analysis

The Pearson's Correlation among variables in Table 5 shows the statistical analysis of this study.

Table 5
Correlation Matric (N =384)

Variable		Cybersecurity Awareness	Analyse	Strategies	Lack of Cybersecurity
Cybersecurity Awareness	Pearson Correlation Sig. (2-tailed) N	1	0.446** <0.001 384	0.406** <0.001 384	0.363** <0.001 384
Analyse	Pearson Correlation Sig. (2-tailed) N	0.446** <0.001 384	1	0.574** <0.001 384	0.488** <0.001 384
Strategies	Pearson Correlation Sig. (2-tailed) N	0.406** <0.001 384	0.574** <0.001 384	1	0.389** <0.001 384
Lack of Cyber Security	Pearson Correlation Sig. (2-tailed) N	0.363** <0.001 384	0.488** <0.001 384	0.389** <0.001384	1

The study uses Pearson's correlation coefficient to assess the relationship between independent variables (Analyse, Strategies, and Lack of Cyber Security) and the dependent variable (Cyber Security Awareness) in Table 5. The results reveal statistically significant positive correlations between all independent variables and Cyber Security Awareness.

The strongest correlation is between Analyse and Cyber Security Awareness ($r = 0.446$, $p < 0.001$), followed by Strategies ($r = 0.406$, $p < 0.001$) and Lack of Cyber Security ($r = 0.363$, $p < 0.001$). These findings indicate that both the analytical and strategic approaches towards cyber security and the perceived lack of it are positively associated with cyber security awareness among bank employees.

The findings from the correlation analysis in Table 5 indicate strong relationships between the variables under study. The most significant association is between the variable "Analyse" and "Cyber Security Awareness", implying that the more emphasis is placed on analysing cyber threats, the more cyber security awareness is demonstrated. This correlation has a coefficient of 0.446, with a significance level of less than 0.001, indicating a strong and significant positive correlation.

Following "Analyse", the following notable correlation is between the variable "Strategies" and "Cyber Security Awareness" with a correlation coefficient of 0.406 ($p < 0.001$). This

relationship suggests that the strategic approaches adopted towards handling cyber security within the organization positively influence the employees' level of cyber security awareness. Finally, the correlation between the variable "Lack of Cyber Security" and "Cyber Security Awareness" is also significant, with a correlation coefficient of 0.363 ($p < 0.001$). This finding implies that the perception of a lack of cyber security within the organization is positively associated with increased cyber security awareness.

The correlations indicate that better analysis of cyber threats, strategic approaches to handling cyber security, and perceived inadequacies in the current cyber security measures are all associated with increased cyber security awareness. The implications of these findings could be significant for banks looking to improve their cyber security awareness and protocols.

The study examines the correlations between various factors and Cyber Security Awareness among bank employees in Malaysia, revealing the following key insights:

Analytical Capabilities and Awareness: The highest correlation is observed between the "Analyse" variable and "Cyber Security Awareness." The strong correlation between the 'Analyse' variable and 'Cyber Security Awareness' suggests that a comprehensive understanding and analysis of cyber threats can significantly enhance cyber security awareness. As such, banks must invest in analytical tools and training to equip employees with the skills to recognize and understand the nature and extent of potential cyber threats.

The Role of Strategic Approaches: The variable "Strategies" also shows a significant positive correlation with "Cyber Security Awareness." This result suggests that strategically handling cyber security, such as implementing robust security policies and regular cyber threat simulations, can effectively improve awareness among bank employees. Banks should therefore prioritize strategic planning in their cyber security efforts.

Impact of Perceived Inadequacies: The correlation between the "Lack of Cyber Security" variable and "Cyber Security Awareness" underscores the influence of perceived security inadequacies on awareness levels. When employees perceive a lack of adequate security measures, their awareness of cyber security issues increases, likely out of necessity. However, this awareness may reflect reactive rather than proactive engagement with cyber security issues. Banks must ensure they have sufficient protective measures and communicate these to their employees to promote informed, proactive engagement with cyber security.

The interplay of Factors: All three independent variables ("Analyse," "Strategies," and "Lack of Cyber Security") show significant correlations with "Cyber Security Awareness," indicating the importance of a multi-faceted approach to improving cyber security in banking. Banks must prioritize thorough risk analysis, strategic planning, and addressing perceived security gaps to foster a robust culture of cyber security awareness among their employees.

In conclusion, these insights provide valuable guidance for banks in Malaysia and potentially globally to bolster their cyber security posture. They highlight the importance of implementing robust security measures and ensuring employees understand these measures and the threats they are designed to combat. Regular training, transparent communication, and strategic planning can promote a culture of cyber security awareness that forms the first line of defence against increasingly sophisticated cyber threats.

Regression Analysis

Table 6

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.502[a]	0.252	0.246	0.55124

a. Predictors: (Constant), Analyse, Strategies and Lack of Cyber Security
b. Dependent Variable: Cyber Security Awareness

The results from the regression analysis are displayed in Table 6. This table shows the R, R Square, Adjusted R Square, and Standard Error of the Estimate for the model. R (multiple correlation coefficient) represents the correlation between the observed and predicted values of the dependent variable. In this model, R is 0.502, indicating a moderate level of correlation. R Square (the coefficient of determination) is the proportion of the variance in the dependent variable that can be predicted from the independent variables. In this model, R Square is 0.252, which suggests that approximately 25.2% of the variation in Cyber Security Awareness can be explained by the independent variables (Analyse, Strategies, and Lack of Cyber Security).

The Adjusted R Square considers the number of predictors in the model and adjusts the R Square accordingly. It is a more accurate measure of the goodness of fit, especially when comparing models with different numbers of predictors. For this model, the Adjusted R Square is 0.246, slightly lower than R Square, indicating that the model can account for nearly 24.6% of the variability in Cyber Security Awareness when adjusting for the number of predictors.

The Standard Error of the Estimate provides a measure of the standard deviation of the error term or residuals, offering an estimate of the accuracy of the predictions. It suggests the average distance that the observed values deviate from the regression line. Lower values of the standard error indicate better precision of the prediction. In this case, the Standard Error of the Estimate is 0.55124.

Table 7

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	38.937	3	12.979	42.712	<.001[b]
	Residual	115.470	380	0.304		
	Total	154.406	383			

a. Dependent Variable: Cyber Security Awareness
b. Predictors: (Constant), Analyze, Strategies and Lack of Cyber Security

Table 7 the ANOVA results demonstrate the significance of the regression model. The regression component has a sum of squares of 38.937, indicating that the predictors collectively contribute to explaining the variation in Cyber Security Awareness. The F-statistic of 42.712 is highly significant ($p < .001$), indicating that the regression model is a good fit for the data. Suggest that the predictors in the model, specifically Analyse, Strategies, and Lack of Cyber Security, strongly influence Cyber Security Awareness among bank employees in Malaysia.

Overall, these findings suggest that the predictors included in the regression model significantly impact the level of Cyber Security Awareness among bank employees in Malaysia. It indicates that factors such as analysis of cyber threats, implementation of strategies, and addressing inadequacies in cyber security contribute to enhancing employees' awareness of cyber security in the banking industry.

Table 8
Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients Beta	t	Sig.
		B	Std. Error			
Variables	(Constant)**	1.541	0.197		7.827	<.0.001
	Analyze	0.227	0.052	0.253	4.375	<.0.001
	Strategies	0.204	0.057	0.197	3.594	<.0.001
	Lack of Cybersecurity	0.176	0.055	0.163	3.178	0.002
**Dependent Variable: Cybersecurity Awareness						

Based on the results presented in Table 8, the regression analysis provides essential insights into the relationship between the predictor variables (Analyse, Strategies, and Lack of Cyber Security) and the dependent variable (Cyber Security Awareness). The coefficient values in the Standardized Coefficients column indicate the strength and direction of the relationship between each predictor variable and Cyber Security Awareness.

Analysing the coefficients showing that Analyse has a standardized coefficient of 0.253, indicating a positive and significant influence on Cyber Security Awareness. This suggests that a one-unit increase in Analyse is associated with a 0.253 standard deviation increase in Cyber Security Awareness. Similarly, Strategies and Lack of Cyber Security have standardized coefficients of 0.197 and 0.163, respectively, indicating positive and significant influences on Cyber Security Awareness. This implies that a one-unit increase in Strategies is associated with a 0.197 standard deviation increase in Cyber Security Awareness. A one-unit increase in Lack of Cyber Security is associated with a 0.163 standard deviation increase.

Based on Table 8 Coefficients, the linear regression equation is as follows

Cyber Security Awareness = 1.541 + 0.227 (Analyse) + 0.204 (Strategies) + 0.176 (Lack of Cyber Security)

In this equation, the constant term (1.541) represents the estimated value of Cyber Security Awareness when all predictor variables (Analyse, Strategies, and Lack of Cyber Security) are set to zero. The coefficients (0.227, 0.204, and 0.176) represent the estimated change in Cyber Security Awareness associated with a one-unit increase in the corresponding predictor variable, holding other predictors constant. Therefore, the equation suggests that Cyber Security Awareness is influenced by the values of the predictors (Analyse, Strategies, and Lack of Cyber Security) as indicated by their respective coefficients.

Discussion

The aim of this study is to investigate the importance of cybersecurity awareness among bank employees and its implications for mitigating cybersecurity risks. Through correlation analysis, this study shows strong positive relationships between cyber security awareness and

various factors, including the level of analysis, implementation of strategies, and the presence of cyber security gaps. The regression analysis further revealed that these factors significantly influenced cyber security awareness among bank employees.

The findings shows that cyber security awareness is crucial in enhancing overall security measures within banks. A one-unit increase in the level of analysis, implementation of strategies, or addressing the lack of cyber security is associated with a corresponding increase in cyber security awareness. This suggests that comprehensive analysis, understanding of cyber threats, and implementing effective strategies significantly enhance cyber security awareness among bank employees.

The implications of the findings are substantial. Firstly, organizations must prioritize cyber security awareness programs and employee training. By investing in continuous education and awareness campaigns, banks can create a security-aware culture where employees can effectively recognize and respond to security threats. This will improve the organization's overall security posture and enhance customer confidence in the bank's ability to safeguard its data.

Secondly, there are some risks associated with bank employees' lack of cyber security awareness. These risks include potential data breaches, phishing attacks, malware infections, and non-compliance with regulatory requirements. The public's awareness of cybersecurity threats and data breach concerns has increased significantly. Research by Quayyum et al (2021) indicates that many affected customers have severed ties with companies or organizations that experienced data breaches, with a majority expressing a loss of trust in the affected bank. These statistics underscore the criticality of implementing security precautions (Corallo et al., 2022). Banks must address these risks by implementing robust security measures, providing tailored training programs, and enforcing policies emphasizing cyber security's importance maintain customer confidence in an increasingly informed consumer base.

Lastly, there is the need for effective strategies to mitigate the issues caused by the lack of cyber security awareness. Cybersecurity education is crucial for organizations to enhance cybersecurity awareness among their staff. When companies prioritize cybersecurity education, employees are more likely to take the necessary steps to reduce cybersecurity threats (Zhang-Kennedy & Chiasson, 2021). A proactive approach to cybersecurity instils greater customer confidence in a bank and increases willingness to work with them. Given that human errors often contribute to cyberattacks, well-trained personnel play a pivotal role in ensuring robust security (Zwilling et al., 2022). Organizations can raise cybersecurity awareness across all levels by implementing a comprehensive security awareness program, empowering employees to recognize security threats and take appropriate actions or escalate them as needed.

Continuous cybersecurity awareness education within enterprises is essential for fostering a security-aware culture. To be more proactive in their cybersecurity measures, organizations must ensure their staff members have access to up-to-date information (Hart et al., 2020). Conducting cybersecurity awareness campaigns can mitigate the likelihood of data breaches and other cybersecurity threats. Through cybersecurity training, employees gain a deeper understanding of safeguarding bank data using standard tools like email, social media, and the Internet. Training programs also teach employees about social engineering techniques such as phishing and spear phishing.

Simulated phishing attacks can be a valuable assessment tool to evaluate users' awareness of cyberattacks and their response to phishing emails. By sending targeted phishing emails that appear legitimate but are harmful, organizations can identify areas where additional training is needed and provide specific guidance (Chang & Coppel, 2020). When employees are well-versed in cybersecurity principles and understand their role in maintaining the bank's security, the risk of a cyberattack occurring and disrupting essential business processes significantly decreases. Security incidents or breaches can lead to substantial financial losses and significant downtime in returning to normal operations (Ansari et al., 2022).

The growing number of regulations corporations must adhere to emphasizes the need to streamline and automate risk management and compliance procedures. Recent research on IT compliance reveals that 83% of respondents prioritize these efforts. Additionally, a survey by Berkman et al (2018) found that 61% of respondents had encountered a cybersecurity or compliance breach in the last three years. Compliance violations related to personal, confidential, or state-secret information are not an option for banks. Mishandling sensitive records can have severe financial consequences for a company's brand and bottom line.

Employees who are unaware of their cybersecurity obligations are more likely to disregard applicable policies and procedures, leading to unintended data exposure or successful cyber-attacks (Bada et al., 2019). One of the significant risks is phishing and malware, often delivered through phishing emails. Spear phishing poses a significant threat, as it involves sending malicious emails that appear to be from legitimate sources according to a survey by CyberEdge. It is unrealistic to expect co-workers to automatically become well-informed about cybersecurity without proper training to combat such attacks (Garba et al., 2020). To effectively combat these risks, employees need a clear understanding of how cybersecurity affects them personally and their careers.

Security awareness training should be tailored to the personnel's specific needs, ideally provided close to the time of crisis (Al Shamsi, 2019). Even if employees are aware of recent utility attacks, they may still need guidance on which attachments to avoid opening or which phishing sites to avoid. Engaging in non-hostile conversations with employees when they raise security concerns is crucial, as these instances can serve as instructional opportunities. Phishing simulators have also shown some effectiveness (Kemper, 2019). However, it is essential to make security awareness training relevant to employees' day-to-day encounters. Since most attacks target employees, their awareness and comprehension of cybersecurity are critical. Employees' lack of awareness makes them easy targets for cybercriminals attempting phishing attacks or social engineering tactics to gain unauthorized access to an organization's network (Kovačević et al., 2020). By ensuring that employees at all levels receive adequate training, organizations can significantly contribute to the success rate of preventing an attack or, at the very least, raising the alarm. This training may include educating employees on recognizing emails tainted with malware and other common attempts at credential theft.

To sustain attention to cybersecurity practices in the long run, organizations should institutionalize training as an integral part of the workplace culture (Moallem, 2018). As the scale of cyber threats is expected to increase exponentially, there is a growing need for professionals with the appropriate knowledge and skills to enter the security industry (Kour & Karim, 2020). Drawing potential candidates and knowledge from academia, research, and the industry becomes crucial to driving growth and meeting current and future demands.

Raising customer awareness about banking security is crucial for mitigating cybersecurity issues. One strategy is to ensure that all bank personnel are knowledgeable about and adhere to bank policies (Corallo et al., 2022). Establishing a solid foundation of policies understood and supported by all staff members is essential for improving cybersecurity in banks. Furthermore, bank employees must use company-approved work equipment, such as desktops, laptops, mobile phones, and tablets, and refrain from using personal devices for banking activities (Corallo et al., 2022).

Educating and training bank workers on phishing fraud can significantly reduce future bank fraud incidents (Zhang-Kennedy & Chiasson, 2021). This strategy has proven effective in enhancing remote security among financial institution workers. While banks are not expected to possess specialized information technology knowledge, employees should be well-informed about email security, as unscrupulous hackers often use phishing techniques and phone calls to obtain personal information (Zwilling et al., 2022).

To strengthen cybersecurity practices, banks should emphasize that visiting online banking sites without SSL certificates is against their policy. Many financial workers use their cell phones for convenience during working hours, but this practice has significantly impacted cybersecurity in financial banks (Hart et al., 2020). Therefore, it is recommended that all financial institutions adopt encrypted apps as essential remote security tools to safeguard communication within the banking industry (Chang & Coppel, 2020).

In conclusion, banks can strengthen their cybersecurity practices and mitigate potential threats by prioritizing awareness programs, addressing risks, and implementing appropriate strategies. Organizations need to recognize the value of continuous education and create a security-conscious culture that protects the institution and its customers.

Acknowledgement

The authors thank UNITAR International University for the publication of this research.

References

Akter, S., Uddin, M. R., Sajib, S., Lee, W. J. T., Michael, K., & Hossain, M. A. (2022). Reconceptualising cybersecurity awareness capability in the data-driven digital economy. *Annals of Operations Research*, pp.1-26.

Al Shamsi, A. A. (2019). Effectiveness of cyber security awareness program for young children: A case study in UAE. *Int. J. Inf. Technol. Lang. Stud*, *3*(2), pp.8-29.

Al-Alawi, A. I., & Al-Bassam, S. A. (2019). Assessing the factors of cybersecurity awareness in the banking sector. *Arab Gulf Journal of Scientific Research*, *37*(4), pp.17-32.

Alita, D., Putra, A. D., & Darwis, D. (2021). Analysis of classic assumption test and multiple linear regression coefficient test for employee structural office recommendation. *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, *15*(3), pp.1-5.

Allen, S., Capkun, S., Eyal, I., Fanti, G., Ford, B. A., Grimmelmann, J., Juels, A., Kostiainen, K., Meiklejohn, S., Miller, A., & Prasad, E., (2020). Design choices for central bank digital currency: Policy and technical considerations (No. w27634). National Bureau of Economic Research.

Al-Shanfari, I., Yassin, W., & Abdullah, R., (2020). Identify factors affecting information security awareness and weight analysis process. *International Journal of Engineering and Advanced Technology (IJEAT)*, *9*(3), pp.534-42.

Amrhein, V., Trafimow, D., & Greenland, S., (2019). Inferential statistics as descriptive statistics: There is no replication crisis if we don't expect replication. *The American Statistician*, *73*(sup1), pp.262-270.

Ansari, M. F., Sharma, P. K., & Dash, B., (2022). Prevention of phishing attacks using AI-based Cybersecurity Awareness Training. *Prevention*.

Astivia, O. L. O., & Zumbo, B. D. (2019). Heteroskedasticity in multiple regression analysis: What it is, how to detect it and how to solve it with applications in R and SPSS. *Practical Assessment, Research, and Evaluation*, *24*(1), p.1.

Bada, M., Solms, S. H., & Agrafiotis, I. (2019). Reviewing national cybersecurity awareness for users and executives in Africa. ArXiv, abs/1910.01005.

Bafadal, I., Juharyanto, J., Nurabadi, A., & Gunawan, I., (2018, October). Principal leadership and its relationship with student learning achievements: A regression analysis. In *3rd International Conference on Educational Management and Administration (CoEMA 2018)* (pp. 156-158). Atlantis Press.

Bai, C., Liao, B. H., & Lei, R. P. (2022). Ethical, legal and social issues raised by human brain banks. European Review for Medical and Pharmacological Sciences, 26(16), pp.5635-5645.

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, *37*(6), pp.508-526.

Bijlsma, A., & Rutledge, L. W. (2020). Information security awareness of bank employees: how differences between headquarters and branch employees affect ISA program design.

Blackwood-Brown, C. G. (2018). *An empirical assessment of senior citizens' cybersecurity awareness, computer self-efficacy, perceived risk of identity theft, attitude, and motivation to acquire cybersecurity skills* (Doctoral dissertation, Nova Southeastern University).

Bonache, J., & Festing, M. (2020). Research paradigms in international human resource management: An epistemological systematisation of the field. *German Journal of Human Resource Management*, *34*(2), pp.99-123.

Chang, L. Y., & Coppel, N. (2020). Building cyber security awareness in a developing country: lessons from Myanmar. *Computers & Security*, *97*, p.101959.

Chua, H. N., Teh, J. S., & Herbland, A. (2021). Identifying the effect of data breach publicity on information security awareness using hierarchical regression. *IEEE Access*, *9*, pp.121759-121770.

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry*, *137*, p.103614.

CyberEdge. (n.d.). Retrieved from https://cyber-edge.com/cdr/

Dharmawansa, A. D., & Madhuwanthi, R. A. M. (2020). Evaluating the Information Security Awareness (ISA) of employees in the banking sector: A case study.

Emerson, R. W. (2021). Convenience sampling revisited: Embracing its limitations through thoughtful study design. *Journal of Visual Impairment & Blindness*, *115*(1), pp.76-77.

Garba, A. A., Siraj**,** M. M., Othman, S. H., & Musa, M. A. (2020). A study on cybersecurity awareness among students in Yobe State University, Nigeria: A quantitative approach. *Int. J. Emerg. Technol*, *11*(5), pp.41-49.

George, D., & Mallery, P. (2003). SPSS for Windows Step by Step: A Simple Guide and Reference. 11.0 Update. 4th ed. Boston: Allyn & Bacon.

George, D., & Mallery, P. (2019). *IBM SPSS statistics 26 step by step: A simple guide and reference*. Routledge.

Gliem, J. A., & Gliem, R. R. (2003). Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales. Midwest Research to Practice Conference in Adult, Continuing, and Community Education, Issue 10, pp. 82-88.

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. *Computers & Security*, *95*, p.101827.

He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., & Tian, X. (2019). Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *Journal of intellectual capital*.

Hoffer, K. J., & Savini, G. (2021). Update on intraocular lens power calculation study protocols: the better way to design and report clinical trials. *Ophthalmology*, *128*(11), pp.e115-e120.

Ivanov, V., Dehtiarov, I., Denysenko, Y., Malovana, N., & Martynova, N. (2018). Experimental diagnostic research of fixture. *Diagnostyka*, *19*.

Jaeger, L., & Eckhardt, A. (2021). Eyes wide open: The role of situational information security awareness for security-related behaviour. *Information Systems Journal*, *31*(3), pp.429-472.

Kam, H. J., Mattson, T., & Goel, S. (2020). A cross industry study of institutional pressures on organizational effort to raise information security awareness. *Information Systems Frontiers*, *22*(5), pp.1241-1264.

Kemper, G. (2019). Improving employees' cyber security awareness. *Computer Fraud & Security*, *2019*(8), pp.11-14.

Kour, R., & Karim, R. (2020). Cybersecurity workforce in railway: its maturity and awareness. *Journal of Quality in Maintenance Engineering*.

Kovacevic, A., Putnik, N., & Toskovic, O. (2020). Factors related to cyber security behavior. *IEEE Access*, *8*, pp.125140-125148.

Lemenkova, P. (2019). Numerical data modelling and classification in marine geology by the SPSS statistics. *International Journal of Engineering Technologies IJET*, *5*(2), pp.90-99.

Lin, H., Zhang, Y., & Liu, X. (2021). Empirical Research on the Quality of Environmental Accounting Information Disclosure based on SPSS. In *Journal of Physics: Conference Series* (Vol. 1769(1), p. 012023). IOP Publishing.

Malaysia Banking System: Number of Employee | Economic Indicators | CEIC. Retrieved January 17, 2023, from https://www.ceicdata.com/en/malaysia/banking-system-indicators/banking-system-no-of-employee

Martin, F., Budhrani, K., & Wang, C. (2019). Examining faculty perception of their readiness to teach online. *Online Learning*, *23*(3), pp.97-119.

Moallem, A. (2018). Cyber security awareness among college students. In *International conference on applied human factors and ergonomics* (pp. 79-87). Springer, Cham.

Mohajan, H. K. (2018). Qualitative research methodology in social sciences and related subjects. *Journal of Economic Development, Environment and People*, *7*(1), pp.23-48.

Newman, M., & Gough, D. (2020). Systematic reviews in educational research: Methodology, perspectives, and application. *Systematic Reviews in Educational Research*, pp.3-22.

Pallant, J. (2016). SPSS Survival Manual: A Step By Step Guide To Data Analysis Using IBM SPSS. 6th ed. London: McGraw Hill Education.

Pallant, J. (2020). SPSS survival manual: A step by step guide to data analysis using IBM SPSS. Routledge.

Prevezianou, M. F. (2020). Beyond ones and zeros: Conceptualizing cyber crises. Risk, Hazards and Crisis in Public Policy, 12(1), 51–72. https://doi.org/10.1002/rhc3.12204

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, *30*, p.100343.

Salleh, K. A., & Janczewski, L. (2019). Security considerations in big data solutions adoption: Lessons from a case study on a banking institution. *Procedia Computer Science*, *164*, pp.168-176.

Sawatsky, A. P., Ratelle, J. T., & Beckman, T. J. (2019). Qualitative research methods in medical education. *Anesthesiology*, *131*(1), pp.14-22.

Scholl, M. (2018). Awareness in information security. *Journal on Systemics, Cybernetics and Informatics* (JSCI), 16(4).

Shrestha, N. (2020). Detecting multicollinearity in regression analysis. *American Journal of Applied Mathematics and Statistics*, *8*(2), pp.39-42.

Utami, Y., Vinsensia, D., & Pangabean, E. (2022). Peningkatan kemampuan mahasiswa dalam menganalisis instrumen pengumpulan data melalui aplikasi SPSS: id. *Aptekmas Jurnal Pengabdian pada Masyarakat*, *5*(3), pp.158-162.

Wakoli, L. W., Ogara, S., & Liyala, S. (2020). An investigation of existing strategies used to counter prevailing cyber threats and vulnerabilities in banks.

Williams, A. S., Maharaj, M. S., & Ojo, A. I. (2019). Employee behavioural factors and information security standard compliance in Nigeria banks. *International Journal of Computing and Digital Systems*, *8*(04), pp.387-396.

Yıldırım, I. (2019). Cyber risk management in banks: Cyber risk insurance. In Global Cyber Security Labor Shortage and International Business Risk (pp. 38-50). IGI Global.

Zhang-Kennedy, L., & Chiasson, S. (2021). A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys (CSUR)*, *54*(1), pp.1-39.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: a comparative study. *Journal of Computer Information Systems*, *62*(1), pp.82-97.