Security Awareness Programs and Behavioral Patterns in Nigeria Deposit Money Banks: Adopting a Robust Cybersecurity Culture.

Francess Okolo*, Arume Tsekiri, Adedayo Sydney Akinsunmi

Texas Southern University & Rice University, Texas, USA

***Corresponding Author**

DOI: https://dx.doi.org/10.47772/IJRISS.2024.806019

Received: 14 May 2024; Accepted: 27 May 2024; Published: 27 June 2024

ABSTRACT

In an era marked by evolving cybersecurity threats, understanding the interplay between Security Awareness Programs, Behavioral Patterns, and Cybersecurity Culture is essential for safeguarding organizational assets and maintaining trust in financial institutions. This study investigated this relationship within Nigeria's Deposit Money Banks, employing a comprehensive analysis of key variables such as Compliance Adherence, Security Policy Acknowledgements, Training Completion Rate, Risk Awareness and Management, Behavioral Analytics, Employee Feedback and Engagement, and Incident Response Time.Utilizing data gathered from a field survey, the study employed multiple regression analysis and tested for hypotheses. Specifically, the study revealed that Compliance Adherence, Training Completion Rate, and Risk Awareness and Management significantly influenced Employee Feedback and Engagement. Compliance Adherence increased Employee Feedback and Engagement by 0.065 (t-stat: 0.750, p = 0.014), Training Completion Rate by 0.397 (t-stat: 3.846, p < 0.001), and Risk Awareness and Management by 0.237 (t-stat: 2.031, p = 0.028). Similarly, Compliance Adherence, Security Policy Acknowledgements, Training Completion Rate, and Risk Awareness and Management significantly impacted Incident Response Time. Compliance Adherence increased Incident Response Time by 0.067 (t-stat: 0.721, p = 0.041), Security Policy Acknowledgements by 0.087 (t-stat: 0.911, p = 0.033), and Training Completion Rate by 0.188 (t-stat: 1.118, p < 0.001). However, Risk Awareness and Management didn't show significant impact on Incident Response Time. Moreover, Compliance Adherence, Security Policy Acknowledgements, Training Completion Rate, and Risk Awareness and Management significantly contributed to Cybersecurity Culture. Compliance Adherence increased Cybersecurity Culture by 0.523 (t-stat: 0.101, p < 0.001), Security Policy Acknowledgements by 0.041 (t-stat: 0.279, p = 0.011), Training Completion Rate by 0.188 (t-stat: 1.139, p < 0.001), and Risk Awareness and Management by 0.239 (t-stat: 1.453, p = 0.041). These findings offered valuable insights for policymakers, bank management, cybersecurity professionals, and employees, informing the development of effective cybersecurity strategies and risk management policies. By understanding the intricate relationship between Security Awareness Programs, Behavioral Patterns, and Cybersecurity Culture, stakeholders could better navigate the complexities of the cybersecurity landscape and safeguard organizational interests.

Keywords: Security Awareness Programs, Behavioral Patterns, Cybersecurity Culture, Compliance Adherence, Security Policy Acknowledgements, Training Completion Rate, Risk Awareness and Management, and Employee Feedback and Engagement

INTRODUCTION

The banking sector is a cornerstone of the global economy; it facilitates financial transactions, drives economic growth, and acts as an intermediary between depositors and borrowers. This function enables individuals and businesses to access the capital needed for various purposes, such as investment, consumption, and business. According to the International Monetary Fund (IMF, 2017), the world's gross domestic product (GDP) is valued at an impressive $79 trillion, with the value of shares trading on stock exchanges nearly matching this figure at $78.2 trillion. These statistics justify the influence of the finance and banking sector on the global economy. In 2024, the projected net interest income in the banking market worldwide is estimated to reach a staggering $10.34 trillion, with traditional banks dominating the market with a projected volume of $8.30 trillion. Despite global economic challenges, the banking sector continues to innovate and adapt to digital transformation, ensuring its resilience and ability to meet customers' evolving needs worldwide (Statista, 2024). According to Dokua Sasu (2022), as of the fourth quarter of 2020, there were over 95,000 bank employees in Nigeria. The behaviors of these employees are essential to banking operations and introducing various products to potential clients, such as savings and current accounts, as well as credit and debit card services. As of 2021, the number of active bank accounts in Nigeria stood at approximately 133.5 million, with savings accounts totaling around 120 million. A notable pattern has been in expanding product offerings and service locations to enhance access to banking services. This includes opening new bank branches and installing an increasing number of automated teller machines (ATMs) and Point-of-Sales (POS) terminals across the country.

The importance of Cybersecurity in the banking industry cannot be overemphasized, particularly in this age characterized by the pervasive influence of digitalization. The evolution of the digital world necessitates the adoption of robust security standards to safeguard organizational business operations effectively (Narayanan, 2024). Financial institutions increasingly rely on third-party services and digital solutions, revolutionizing traditional banking operations and customer interactions (Financier Worldwide Magazine, 2014). However, alongside these advancements, the pervasive nature of digital technology has ushered in a surge in cybercrime, posing significant threats to the integrity and security of the banking sector. Reports indicate that cybercriminals have illicitly accessed over half of the world's top 50 banking websites over the past decade, resulting in approximately $1 billion in annual losses within the banking industry alone (Financier Worldwide Magazine, 2014). The sophisticated tactics employed by cybercriminals, coupled with the interconnectedness of the global financial sector, underscore the critical need for robust cybersecurity measures to safeguard against potential breaches and mitigate the resulting financial and reputational risks. Within the Nigerian banking sector, the alarming rise of cybercrime is evident, attributed to the rapid expansion of the information and communication technology (ICT) environment and the nation's push towards a cashless economy (Ojeka & Egbide, 2017). These cyber threats extend beyond financial damages, encompassing reputational damage, discouragement of foreign investment, and incalculable human misery and tragedy. Nigerian banks have incurred staggering losses amounting to NGN 159 billion between 2000 and 2013 and an annual loss of NGN 413 billion (USD 2.5 billion) to cybercrime, highlighting the imperative to enhance cybersecurity measures for national security and economic well-being (Ojeka & Egbide, 2017).

The growing significance of security awareness programs and behavioral patterns in enhancing cybersecurity in the bank industry is increasingly evident in today's digital landscape. While technological advancements have bolstered defenses against cyber threats, the human element remains a critical vulnerability (Andronache, 2021). This justifies the centrality of human roles in cybersecurity policy, awareness, and training, as these factors play pivotal roles in protecting organizational information, assets, and people. Research indicates that organizational resilience hinges on employees' perceptions of formal security measures and informal cultural norms (Andronache, 2021). Moreover, studies highlight the stark contrast in security awareness between trained and untrained individuals, emphasizing the effectiveness of education and training initiatives in raising awareness levels (Hammarstrand & Fu, 2015). However, increasing awareness may not suffice, as behavioral changes and proactive security measures are equally crucial (Hammarstrand & Fu, 2015). Consequently, there is a pressing need to look deeper into the behavioral aspects of cybersecurity, considering that the majority of cyber incidents stem from human factors (Maalem Lahcen et al., 2020). In light of these challenges, this research aims to investigate the role of security awareness programs and behavioral patterns in shaping cybersecurity culture within the Nigerian deposit money banks.

In recent studies within the Nigerian banking sector, behavioral factors have emerged as important determinants of organizational outcomes, such as employee engagement and information security standard compliance. Nwairoegbu-Agbam (2020) investigated the relationship between behavioral cultural competency and organizational identification in Deposit Money Banks. The study found a significant association between cultural competency and organizational loyalty and membership. This justifies the importance of recognizing and addressing diversity-based issues within organizational settings. Williams et al. (2019) explored the impact of behavioral factors on information security standard compliance. They found that factors such as security awareness and normative beliefs positively influence compliance with international security standards.

Moreover, Agbeche (2021) looked into the relationship between cyber security awareness and corporate agility of Deposit Money Banks in Nigeria, emphasizing the importance of heightened awareness and proactive measures in combating cyber threats. The study underlines the need for training initiatives and enhanced awareness among bank employees and clients to effectively address emerging cyber threats. These findings emphasize the significance of prioritizing cyber security awareness initiatives to foster a culture of vigilance and responsiveness within banking organizations. Krishnan et al. (2023) emphasized the importance of enhancing cybersecurity awareness among banking employees in Malaysia, highlighting the necessity of providing robust training and fostering a culture of awareness to mitigate cyber risks effectively. These studies spotlight the important role of employee behavioral factors, including cultural competency and security awareness, in shaping organizational outcomes within the banking sector. However, there remains a gap in understanding the specific relationship between security awareness programs, behavioral patterns, and cybersecurity culture within Nigeria's deposit money banks. Hence the justification for the first hypothesis of this study.

Hypothesis 1 Security awareness and behavioral patterns have no significant effect on employee feedback and engagement in Nigeria's deposit money banks.

Scholars have delved into the role of cybersecurity in driving financial innovation and mitigating cyber threats within the Nigerian banking sector. Akintoye et al. (2022) examined how cybersecurity influences the economic innovation of Deposit Money Banks (DMBs) in Nigeria, finding a statistically significant positive relationship between cybersecurity, represented by risk management and bank monitoring, and financial innovation in DMBs. Fatoki (2023) investigated the influence of cybersecurity on financial fraud in the Nigerian banking industry, highlighting prevalent electronic frauds like computer viruses, hacking, phishing, and pharming. These occurrences were attributed to factors such as insufficient data encryption and collusion between employees and external parties. While proposing solutions like security audits and multi-factor authentication, the study highlighted the substantial financial losses and decreased productivity resulting from cyber fraud incidents. However, to comprehensively understand the dynamics at play, further exploration is needed regarding the specific impact of security awareness programs and behavioral patterns on incidence response time within Nigerian deposit money banks. Thus, this study's second hypothesis aims to address this gap by examining whether security awareness and behavioral patterns significantly affect incidence response time in Nigerian deposit money banks.

Hypothesis 2 Security awareness and behavioral patterns have no significant effect on incidence response time in the Nigeria deposit money bank.

The primary objective of this study is to investigate the effect of security awareness programs, measured by compliance adherence, security policy acknowledgments, and training completion rate, along with behavioral patterns, assessed through risk awareness and management and behavioral analytics, on cybersecurity culture within the Nigerian deposit money bank. This research aims to comprehensively understand how these independent variables influence the dependent variable, cybersecurity culture, measured by employee feedback and engagement and incident response time. By examining the interplay between security awareness initiatives, behavioral tendencies, and their impact on cybersecurity culture, this study seeks to be valuable in enhancing cyber resilience and safeguarding the integrity of the banking sector in Nigeria.

LITERATURE REVIEW

Conceptual Review

Cybersecurity Culture encompasses the collective knowledge, beliefs, perceptions, attitudes, assumptions, norms, and values of individuals regarding cybersecurity and its integration into their behavior with information technologies (Uchendu et al., 2021). It has to do with making information security an inherent part of an employee's job, habits, and conduct, embedding security practices into the fabric of organizational culture (Martins & Eloff, 2002). This holistic approach fosters a mindset where cybersecurity is viewed as an integral component of organizational operations, emphasizing the importance of instilling security awareness, promoting risk perception, and nurturing a closely knit organizational culture that prioritizes cybersecurity (Ross & Masters, 2011; McKinsey, 2011; Post & Kagan, 2007). A resilient CSC develops naturally from the behaviors and attitudes of employees towards information assets at work, improving resilience against cyber threats, especially those initiated through social engineering (Ponemon Institute, 2012; Fagerström, 2013). Organizations must actively maintain and adapt their CSC in response to evolving technologies, threats, and changing organizational structures (Ngo, 2008). This approach fosters a culture of security consciousness, empowering individuals to make informed security decisions and ultimately contributing to enhanced cyber resilience and organizational security posture.

The concept of Security awareness programs is important in educating employees, contractors, partners, and other stakeholders on safeguarding sensitive information from cyber threats and maintaining the security of digital assets (Security Awareness Training 101, 2024). These programs inform participants on how to recognize and mitigate common cyber threats, such as phishing emails and malicious attachments, thereby reducing the risk related to human vulnerabilities in cybersecurity (Gardner & Thomas, 2014). By establishing a security-aware culture across all business units, organizations can strengthen information security and ensure compliance with data privacy regulations. The CISA Cybersecurity Awareness Program, a national public awareness effort, emphasizes the shared responsibility of cybersecurity and aims to empower individuals to adopt safer online behaviors (CISA Cybersecurity Awareness Program, 2024). Through the dissemination of simple, easy-to-understand resources and tips, this program strives to enhance cybersecurity awareness among Americans and promote secure online practices. Effective security awareness planning is essential for the success of these programs, requiring clear cybersecurity goals, performance metrics, and strategies to boost employee participation and completion rates.

Compliance adherence within organizational cybersecurity frameworks is paramount for ensuring the alignment of individuals' actions with established security policies, procedures, and regulations, thus mitigating risks and safeguarding sensitive information (CompTIA, 2022). It involves adhering to standards and regulatory requirements mandated by governing bodies to protect the confidentiality, integrity, and availability of information, whether stored, processed, integrated, or transferred (Cybersecurity Compliance, 2022). Cybersecurity compliance serves as a risk management method, guiding organizations in implementing systematic governance approaches to minimize the likelihood of breaches and ensure data confidentiality. By adopting a security-first approach and integrating pre-defined security measures and controls, organizations can mitigate potential cyber threats and adhere to national and state-level cyber laws.

Theoretical Framework

The study's theoretical framework draws upon Social Learning Theory (SLT), the Theory of Planned Behavior (TPB), and the Protection Motivation Theory (PMT). Social Learning Theory (SLT), proposed by Albert Bandura, is highly relevant in understanding how individuals learn cybersecurity practices within organizational settings. Bandura's theory emphasizes observational learning, whereby individuals acquire knowledge, skills, attitudes, and beliefs by observing the behaviors of others and the consequences that follow (McLeod, 2011). SLT posits that people learn through direct experiences and observing others, modeling their behaviors, and imitating them (Bandura, 1977). This theory highlights the importance of attention, retention, reproduction, and incentives in the learning process (Lelchook & de Luque, 2015). In cybersecurity, SLT suggests that employees learn security practices by observing their peers, superiors, or security experts within the organization. By paying attention to these models and understanding the consequences of their actions, employees internalize cybersecurity practices and incorporate them into their daily routines. This highlights the significance of providing effective security awareness training and role modeling behaviors that promote compliance adherence (Mobley & Sandovel, 2008).

The Theory of Planned Behavior (TPB), developed by Ajzen (1991), posits that behaviors are influenced by intentions, which are determined by three main factors: attitudes, subjective norms, and perceived behavioral control. In the context of cybersecurity, this theory suggests that individuals' intentions to comply with information security policies are influenced by their attitudes towards security practices, subjective norms regarding social pressures and expectations related to security compliance, and perceived behavioral control, which encompasses factors such as self-efficacy and external constraints. For instance, Sommestad et al. (2017) applied TPB to examine information security policy compliance and found that individuals' intentions to comply were influenced by their attitudes towards security measures, social norms within the organization, and their perceived ability to adhere to security policies. External factors may also directly impact behavior, depending on the individual's perceived control. However, TPB assumes that individuals act rationally based on these factors, though they may not always consciously consider them during decision-making processes. This theory provides valuable insights into understanding and predicting individuals' compliance behaviors within organizational cybersecurity frameworks.

Protection Motivation Theory (PMT) offers a valuable framework for understanding individuals' motivations to protect themselves from perceived threats, making it particularly relevant in the context of cybersecurity. According to Rogers (1975), PMT comprises three crucial components: the magnitude of the noxiousness of a depicted event, the probability of that event's occurrence, and the efficacy of a protective response. These components initiate corresponding cognitive appraisal processes that mediate attitude change. Shillair (2020) further elaborates on PMT, stating that individuals evaluate potential responses through threat appraisal and coping appraisal processes. The threat appraisal involves assessing the severity and likelihood of the threat, while the coping appraisal considers the efficacy of the response, response cost, and perceived self-efficacy. If the threat appraisal outweighs the coping appraisal, maladaptive responses such as denial may occur, whereas stronger coping responses lead to protection motivation. The study by Briggs et al. (2017) emphasizes the importance of understanding and improving both threat and coping appraisals to shift behavioral patterns from inaction to action. Tunner Jr. et al. (1989) highlights the effectiveness of incorporating coping response information into fear appeals, as it influences the adoption of appropriate coping behaviors.

Empirical Review

The empirical studies thoroughly review the Security awareness programs and behavioral patterns in Nigeria deposit money banks. Exploring the dynamics between cybersecurity practices and the banking sector and focusing on how different studies have illuminated the relationship between cybersecurity measures and financial industry resilience. In a study conducted by Agbeche Aaron's study on Cyber Security Awareness and Corporate Agility of Deposit Money Banks in Nigeria, he looks into the importance of cyber security awareness in today's digital landscape. The study highlights the challenges faced by DMBs in managing cyber security solutions, such as difficulty tracing cyber-crime attackers, limited cybercrime laws, and inadequate IT security knowledge among internet users (Aaron, 2021). By employing the Theory of Protection Motivation, the study emphasizes the significance of fostering cyber security awareness to combat increasing threats to personal and corporate information. Recommendations include the introduction and enforcement of cybercrime laws, along with training and awareness programs for DMB staff and clients. Bako, together with other scholars, researched The Effects of Organizational Culture on Employees' Job Performance Among Selected Deposit Money Banks (DMBs) in Gombe State, Nigeria. They explore the relationship between organizational culture and employee productivity in DMBs. While not directly focused on cybersecurity, this study sheds light on factors influencing employee performance, which is crucial for understanding behavioral patterns in organizational settings. The findings suggest a negative correlation between certain training methods and the productivity of DMBs. This finding justifies the importance of adopting effective training techniques to enhance employee performance (Bako et al., 2024). Also, Adeloye (2024) affirmed the significance of technological integration in mitigating fraud risks, expediting claims processing, and enhancing communication.

A Nwairoegbu-Agbam study on Behavioural Cultural Competence and Organizational Identification in Deposit Money Banks in Rivers and Bayelsa States in Nigeria examines the relationship between behavioral cultural competency and organizational identification in DMBs. While not directly addressing cybersecurity, this study contributes to understanding organizational dynamics and employee behavior within DMBs. The findings indicate a significant relationship between behavioral cultural competency and organizational identification, emphasizing the importance of fostering a positive organizational culture to enhance employee loyalty and membership (Nwairoegbu-Agbam, 2020). Okolo (2023) considered a secondary data by investigating the effect of National security in the United states.

Ajufo and Qutieshat (2023) shed light on the human factors influencing cybersecurity in Nigerian banks. They identify social engineering, poor information security culture, risky password practices, stress, burnout, and security fatigue as critical factors contributing to successful cyber-attacks. The study emphasizes the importance of cybersecurity awareness and training in mitigating these human-related vulnerabilities, providing practical recommendations for Nigerian banks to enhance their cybersecurity posture. Rufus Akintoye et al. (2022) explore the impact of cybersecurity on financial innovation in Nigerian deposit money banks. Their findings reveal a statistically significant positive relationship between cybersecurity, proxied by risk management and bank monitoring, and financial innovation. The study highlights the importance of robust risk management frameworks and proactive monitoring of e-banking channels to foster financial innovation while safeguarding against cyber threats. Hassan et al. (2024) provide a comprehensive overview of cybersecurity practices in the global banking industry, with a specific focus on Nigerian banks. They highlight the escalating frequency and sophistication of cyber threats faced by financial institutions worldwide, necessitating robust cybersecurity frameworks. The study examines cybersecurity practices adopted by Nigerian banks, including regulatory compliance, incident response mechanisms, and collaborative initiatives with international cybersecurity entities. It emphasizes the importance of public awareness campaigns and collaborative efforts in fostering a cyber-resilient banking environment in Nigeria.

MATERIALS AND METHOD

The research design adopted for this study is a survey research design. Because it allows for collecting well-informed perspectives on the effect of Security Awareness Programs and Behavioral Patterns on

Cybersecurity Culture in Nigeria's Deposit Money Banks. The study focuses on independent variables, including Security Awareness Programs, measured with Compliance Adherence, Security Policy Acknowledgements, and Training Completion Rate. And Behavioral Patterns, which involves Risk Awareness and Management and Behavioral Analytics. The dependent variable is Cybersecurity Culture, encompassing Employee Feedback and Engagement and Incident Response Time. The population of interest is 33 banks drawn from the list of deposit banks in Nigeria (CBN, 2021), categorized into various licenses, such as commercial bank licenses with international, national, and regional authorizations, as well as non-interest banking licenses and merchant banking licenses. To ensure representation, the study focused on 17 banks holding commercial banking licenses with international authorization (8 banks) and national authorization (11 banks), based on data from the Central Bank of Nigeria (CBN, 2021). A stratified and purposive sampling technique selected 11 banks from these categories. The questionnaire is distributed randomly among the staff of the selected banks. The study achieved a sample size of 400 participants with a convenience sampling approach.

Data Collection

Data collection involves using a structured questionnaire to capture relevant information from bank employees and security personnel on Security Awareness Programs and Behavioral Patterns in Cybersecurity Culture. The distribution of the questionnaire was randomized among the selected participants. Multiple linear regression analysis was utilized for data analysis. This statistical technique enables the examination of the relationship between multiple independent variables, security awareness programs, behavioral patterns, and a dependent variable, which in this study is the cybersecurity culture within Nigeria's deposit money banks. The measurement of the variable is displayed in Table 1.

Table 1: Measurement of Variable

S/N	Variable Name	Definition	Measurement	Supporting Literature	Source of Data
1	Security Awareness Programs	Programs aimed at enhancing awareness of security measures and protocols within the organization	Compliance Adherence, Security Policy Acknowledgements, Training Completion Rate	Andronache (2021); Hammarstrand & Fu (2015)	Survey
	Compliance Adherence	The degree to which employees adhere to security compliance standards	Compliance Adherence	Williams et al. (2019)	Survey
	Security Policy Acknowledgements	Employees' acknowledgment and understanding of organizational security policies and procedures	Security Policy Acknowledgements	Narayanan (2024)	Survey
	Training Completion Rate	Rate of completion of cybersecurity training among employees	Training Completion Rate	Krishnan et al. (2023)	Survey

2	Behavioral Patterns	Observable behavioral trends and patterns related to security awareness and risk management	Risk Awareness and Management Behavioral Analytics	Andronache (2021); Fatoki (2023)	Survey
	Risk Awareness and Management	Employee awareness and management of cybersecurity risks	Risk Awareness and Management	Akintoye et al. (2022); Fatoki (2023)	Survey
	Behavioral Analytics	Analysis of employee behavior related to cybersecurity incidents and responses	Historical incident logs, incident reports, survey responses	Krishnan et al. (2023); Akintoye et al. (2022)	Survey
3	Cybersecurity Culture	The prevailing attitudes, beliefs, and behaviors of employees towards cybersecurity within the organization	Employee Feedback Engagement; Incident Response Time	Narayanan (2024); Agbeche (2021)	Survey
	Employee Feedback and Engagement	Employees' level of involvement, satisfaction, and communication regarding cybersecurity policies and practices	Employee Feedback and Engagement	Williams et al. (2019); Nwairoegbu-Agbam (2020)	Survey
	Incident Response Time	The time taken by the organization to respond to cybersecurity incidents and breaches	Incident Response Time	Akintoye et al. (2022); Fatoki (2023)	Survey

Source: Author's Compilation, (2024).

Reliability Test

A reliability test was conducted on all proxies of security awareness, behavioral patterns, and cybersecurity culture. As part of the study, 10% of the total sample size, equivalent to 40 copies of the questionnaire, were distributed among selected banks, which were outside the study scope. The results indicated that all questions used for the analysis were deemed appropriate without requiring revision, as the coefficient value exceeded 0.70. Cronbach's alpha coefficient measures the reliability of the measurement scales for both independent and dependent variables was assessed using. The reliability test results have presented in Table 2 indicate high levels of internal consistency for all variables. For the independent variables, including Security Awareness Programs, Compliance Adherence, Security Policy Acknowledgements, Training Completion Rate, Behavioral Patterns, Risk Awareness and Management, and Behavioral Analytics, Cronbach's alpha coefficients ranged from 0.701 to 0.882. This figure signifies excellent to good reliability. Similarly, the dependent variables, Cybersecurity Culture, Employee Feedback and Engagement, and Incident Response Time has excellent reliability with Cronbach's alpha coefficients ranging from 0.803 to 0.921. These values means that the measurement scales are reliable and consistent in capturing the intended constructs, thereby indicating no need for revision.

Table 2: Reliability Test

S/N	Variables	No of items	Cronbach's Alpha Coefficient	Remarks	Recommendation
Independent Variable	**Security Awareness Programs**	**15**	**0.882**	**Excellent**	**No revision is required**
	compliance adherence	5	0.831	Excellent	No revision is required
	security policy	5	0.873	Excellent	No revision is required
	training completion rate	5	0.779	Good	No revision is required
	Behavioural Patterns	**10**	**0.765**	**Good**	**No revision is required**
	Risk Awareness and management	5	0.818	Excellent	No revision is required
	Behavioral analytics	5	0.701	Good	No revision is required
Dependent Variable	**Cybersecurity Culture**	**10**	**0.899**	**Excellent**	**No revision is required**
	Employee feedback and engagement	5	0.803	Excellent	No revision is required
	Incident response time	5	0.921	Excellent	No revision is required

Source: Author's Computation, 2024; data from Field Survey

Models Specification

The model specification will explain the effect of Security Awareness Programs and Behavioral Patterns on Cybersecurity Culture in Nigeria's Deposit Money Banks. The models will be specified thus:

$$EFM_{i} = \beta_{\circ} + \beta_1 CP + \beta_2 SCP + \beta_3 TCR + \beta_4 RKM + \varepsilon_{i} - - - - - - - - - Model\ 1$$

$$IRT_{i} = \beta_{\circ} + \beta_1 CP + \beta_2 SCP + \beta_3 TCR + \beta_4 RKM + \varepsilon_{i} - - - - - - - - - Model\ 2$$

$$CSC_{i} = \beta_{\circ} + \beta_1 CP + \beta_2 SCP + \beta_3 TCR + \beta_4 RKM + \varepsilon_{i} - - - - - - - - - Main\ Model$$

Where:

While β_1, β_2, β_3, β_4 are the coefficients of the explanatory variables

Where:

CPH: Compliance Adherence

SCP: Training Completion Rate

TCR: Training Completion Rate

RKM: Risk Awareness and Management

BHA: Behavioral Analytics

EFM: Employee Feedback and Engagement

IRT: Incident Response Time

CSC: Cybersecurity Culture

εi = Error term

RESULTS AND DISCUSSION

To investigate the relationships between Security Awareness Programs, Behavioral Patterns, and Cybersecurity Culture in Nigeria’s Deposit Money Banks, Multiple regression will be employed Multiple regression is a widely-used statistical technique for examining the impact of multiple independent variables on a single dependent variable. Statistical software STATA was utilized for regression analysis. A reliability test will be conducted to test for the validity of the constructs. The results of the regression analysis will provide insights into the extent to which Security Awareness Programs (Compliance Adherence, Security Policy Acknowledgements, Training Completion Rate) and Behavioral Patterns (Risk Awareness and Management, Behavioral Analytics) influence Cybersecurity Culture (Employee Feedback and Engagement, Incident Response Time) in Nigeria’s Deposit Money Banks. This will contribute immensely to the formulation of effective cybersecurity strategies and risk management policies.

Response Rate

Table 3 presents the response rate obtained during the survey. Out of the 400 distributed questionnaires, 356 completed and usable copies were returned, representing an 89.00% response rate. Meanwhile, 44 questionnaires were either unreturned or incomplete, constituting an 11.00% non-response rate.

Table 3: Response Rate

Category	**Frequency N**	**Percentage (%)**
Completed usable copies of questionnaire	356	89.00
Unreturned/incomplete copies of questionnaire	44	11.00
Total	**400**	**100**

Source: Author’s Computation, 2024; data from Field Survey

Socio-demographic Characteristics of the respondents

Table 4 presents the socio-demographic characteristics of the respondents. Regarding educational background, most respondents held NCE/OND/HND qualifications, comprising 53.09% of the sample, followed by those with Bachelor’s degrees at 28.37%, and individuals with Master’s degrees at 18.54%. Regarding age distribution, the highest proportion falls within the range of 27 to 34 years, accounting for 52.53%, while 20 to 26-year-olds represent 18.82%. For years of experience, the largest group consists of respondents with 5 to 10 years of experience, constituting 46.07%, followed by those with less than 5 years at 27.53%, and 11 to 15 years at 23.87%. Respondents with over 15 years of experience are the smallest group, making up only 2.53% of the sample.

Table 4: Socio-Demographic Characteristics

Socio-demographic Characteristics	**Frequency Distribution**	**Percentage Distribution**
Educational		
NCE/OND/HND	189	53.09

Bachelor's degree	101	28.37
Master's Degree	66	18.54
Age of the Variable		
20 – 26	67	18.82
27 – 34	187	52.53
35 – 43	70	19.66
> 43	32	8.99
Year of experience		
< 5 year(s)	98	27.53
5 – 10	164	46.07
11 – 15	85	23.87
> 15 years	9	2.53

Source: Author's Computation, 2024; data from Field Survey

Bivariate and Multicollinearity Test

Table 5 presents the correlation matrix and multicollinearity test results for the variables under study. The correlation coefficients range from -1.000 to 1.000, with values closer to 1 indicating a stronger positive correlation and values closer to -1 indicating a stronger negative correlation. Compliance Adherence shows a moderate positive correlation with Security Policy (r = 0.430) and Training Completion Rate (r = 0.339), while it has a weak positive correlation with Behavioral Analytics (r = 0.611). Security Policy has a moderate positive correlation with Behavioral Analytics (r = 0.420) and Employee Feedback and Engagement (r = 0.511). Training Completion Rate displays a moderate positive correlation with Security Policy (r = 0.643) and a weak positive correlation with Employee Feedback and Engagement (r = 0.591). Risk Awareness and Management exhibit weak positive correlations with Compliance Adherence (r = 0.288) and Security Policy (r = 0.571). Behavioral Analytics shows a moderate positive correlation with Compliance Adherence (r = 0.420) and a weak positive correlation with Employee Feedback and Engagement (r = 0.411). Incident Response Time demonstrates a weak negative correlation with Security Policy (r = -0.543) and a weak positive correlation with Risk Awareness and Management (r = 0.568).

Variance Inflation Factor (VIF) and tolerance levels are used to assess multicollinearity among the variables. VIF values greater than 10 indicate the presence of multicollinearity, while tolerance levels closer to 0 suggest higher multicollinearity. The VIF values for all variables are below 10, ranging from 1.02 to 2.38, indicating no significant multicollinearity concerns. Also, tolerance levels ranging from 0.420 to 0.980 indicate an adequate level of independence among the variables, further supporting the absence of multicollinearity issues.

Table 5: Correlation and Multicollinearity Test

Variables	compliance adherence	security policy	training completion rate	Risk Awareness and management	Behavioral analytics	Employee feedback and engagement	Incident response time	VIF	1/VIF
Compliance adherence	1.000							1.02	0.980

Security policy	0.430	1.000						1.55	0.645
Training completion rate	0.339	0.643	1.000					2.38	0.420
Risk Awareness and management	0.288	0.571	-0.411	1.000				1.95	0.513
Behavioral analytics	0.611	0.420	0.329	0.541	1.000			1.76	0.568
Employee feedback and engagement	0.328	0.511	0.591	0.432	0.411	1.000			
Incident response time	0.408	-0.543	0.391	0.568	0.182	0.348	1.000		

Where VIF indicates variance inflation factor; 1/VIF – tolerance level.

Source: Author’s Computation, 2024; data from Field Survey

Inferential Analysis

Research Hypothesis 1: Security awareness and behavioural pattern has no significant effect on Employee feedback and engagement in the Nigeria deposit money bank.

$$EFM_{\mathrm{i}} = \beta_{\circ} + \beta_1 CP + \beta_2 SCP + \beta_3 TCR + \beta_4 RKM + \varepsilon_{\mathrm{i}} --------- Model\,1$$

$$EFM_{\mathrm{i}} = 1.002 + 0.065CP + 0.011SCP + 0.397TCR + 0.237RKM + \varepsilon_{\mathrm{i}}$$

Table 6: Security Awareness program and behavoural pattern on Employee feedback and engagement

Model	B	SE	t-stat	Sig.	ANOVA (Sig.)	R	Adjusted R^2	F (5,350)
(Constant)	1.002	0.143	4.116	.000	0.000b	0.689	0.648	11.315
CPH	0.065	0.080	0.750	0.014				
SCP	0.011	0.013	0.432	0.031				
TCR	0.397	0.077	3.846	0.000				
RKM	0.237	0.032	0.4331	0.028				
BHA	0.541	0.084	1.534	0.116				
	Predictors: (Constant). CPH, SCP, TCR, RKM, BHA							
	Dependent Variable: EFM							

Source: Author’s Computation, 2024; data from Field Survey

Hypothesis one of Table 6 of this study aimed to investigate the effect of Security Awareness Programs and Behavioral Patterns on Employee Feedback and Engagement in Nigeria’s deposit money banks. The results indicate that Compliance Adherence (CPH), Training Completion Rate (TCR), and Risk Awareness and Management (RKM) demonstrate statistically significant positive relationships with Employee Feedback and Engagement. Specifically, a one-unit increase in Compliance Adherence leads to a 0.065 increase in Employee Feedback and Engagement, with a significant t-statistic of 0.750 (p = 0.014). Similarly, Training Completion Rate shows a positive relationship, with a one-unit increase resulting in a 0.397 increase in Employee Feedback and Engagement, supported by a significant t-statistic of 3.846 (p < 0.001). Risk Awareness and Management also exhibits a positive effect, with a one-unit increase associated with a 0.237 increase in Employee Feedback and Engagement, supported by a significant t-statistic of 2.031 (p = 0.028). However, Security Policy (SCP) and Behavioral Analytics (BHA) do not show statistically significant effects on Employee Feedback and Engagement.

The adjusted R-squared value for the model is 0.648, indicating that approximately 64.8% of the variability in Employee Feedback and Engagement is explained by the included independent variables. Individually, Compliance Adherence (CPH), Training Completion Rate (TCR), and Risk Awareness and Management (RKM) are statistically significant at the 5% level, while Security Policy (SCP) and Behavioral Analytics (BHA) are not. The F-statistic of 11.315 (p < 0.000) suggests that the combined effects of the independent variables are statistically significant in explaining Employee Feedback and Engagement.

Therefore, based on the significance of the F-statistic and the rejection of the null hypothesis, it can be concluded that Security Awareness Programs and Behavioral Patterns have a significant effect on Employee Feedback and Engagement in Nigeria's deposit money banks.

Research Hypothesis 2: Security awareness and behavioural pattern has no significant effect on incidence response time in the Nigeria deposit money bank.

$$IRT_{\mathrm{i}} = \beta_{\circ} + \beta_1 CP + \beta_2 SCP + \beta_3 TCR + \beta_4 RKM + \varepsilon_{\mathrm{i}} --------- Model\ 2$$

$$IRT_{\mathrm{i}} = 1.616 + 0.067CP + 0.087SCP + 0.188TCR + 0.143RKM + \varepsilon_{\mathrm{i}}$$

Table 7: Security Awareness program and behavoural pattern on incident response time

Model	B	SE	t-stat	Sig.	ANOVA (Sig.)	R	Adjusted R^2	F (5,350)
(Constant)	1.616	0.355	4.116	0.000	0.009^b	0.865	0.853	8.677
CPH	0.067	0.067	0.721	0.041				
SCP	0.087	0.088	0.911	0.033				
TCR	0.188	0.055	1.118	0.000				
RKM	0.143	0.653	0.764	0.007				
BHA	0.061	0.011	.881	0.019				
	Predictors: (Constant). CPH, SCP, TCR, RKM, BHA							
	Dependent Variable: IRT							

Source: Author's Computation, 2024; data from Field Survey

Table 7 posited that Security Awareness Programs and Behavioral Patterns have no significant effect on Incident Response Time in Nigeria's deposit money banks. The results from Model 2 suggest that Compliance Adherence (CPH), Security Policy (SCP), Training Completion Rate (TCR), and Behavioral Analytics (BHA) demonstrate statistically significant effects on Incident Response Time (IRT), while Risk Awareness and Management (RKM) does not exhibit a statistically significant effect.

Specifically, Compliance Adherence (CPH) shows a positive relationship with Incident Response Time, with a one-unit increase resulting in a 0.067 increase in IRT, supported by a significant t-statistic of 0.721 (p = 0.041). Security Policy (SCP) demonstrates a positive relationship, with a one-unit increase leading to a 0.087 increase in IRT, supported by a significant t-statistic of 0.911 (p = 0.033). Training Completion Rate (TCR) also exhibits a positive effect on Incident Response Time, with a one-unit increase associated with a 0.188 increase in IRT, supported by a significant t-statistic of 1.118 (p < 0.001). However, Risk Awareness and Management (RKM) does not demonstrate a statistically significant effect on Incident Response Time. Behavioral Analytics (BHA) also shows a statistically significant effect on IRT, with a one-unit increase resulting in a 0.061 increase in IRT, supported by a significant t-statistic of 0.881 (p = 0.019).

The adjusted R-squared value for Model 2 is 0.853, indicating that the included independent variables explain approximately 85.3% of the variability in Incident Response Time. The F-statistic of 8.677 (p < 0.000) suggests that the combined effects of the independent variables are statistically significant in explaining Incident Response Time.

Therefore, based on the significance of the F-statistic and the rejection of the null hypothesis, it can be concluded that Security Awareness Programs and Behavioral Patterns significantly affect Incident Response Time in Nigeria's deposit money banks.

Main Hypothesis: Security awareness program and behavioural pattern have no significant effect on cybersecurity culture in the Nigeria deposit money bank.

$$CSC_{i} = \beta_{\circ} + \beta^{1}CP + \beta^{2}SCP + \beta^{3}TCR + \beta^{4}RKM + \varepsilon_{i} --------- Main\ Model$$

$$CSC_{i} = 1.281 + 0.53CP + 0.041SCP + 0.188TCR + 0.239RKM + \varepsilon_{i}$$

Table 4.6 Security Awareness program and behavoural pattern on cybersecurity Culture

Model	B	SE	t-stat	Sig.	ANOVA (Sig.)	R	Adjusted R^2	F (5,350)
(Constant)	1.281	0.078	4.140	0.000	0.011^{b}	0.847	0.831	16.144
CPH	0.523	0.055	0.101	0.000				
SCP	0.041	0.046	0.279	0.011				
TCR	0.188	0.053	1.139	0.000				
RKM	0.239	0.156	1.453	0.041				
BHA	0.178	0.054	1.831	.089				
	Predictors: (Constant). CPH, SCP, TCR, RKM, BHA							
	Dependent Variable: CSC							

Source: Author's Computation, 2024; data from Field Survey

The main hypothesis of this study aimed to examine the impact of Security Awareness Programs and Behavioral Patterns on Cybersecurity Culture (CSC) in Nigeria's deposit money banks. Model 3 provides insights into the relationship between the independent variables (Compliance Adherence, Security Policy, Training Completion Rate, Risk Awareness and Management, and Behavioral Analytics) and the dependent variable (Cybersecurity Culture).

Starting with Compliance Adherence (CPH), the coefficient estimate suggests that a one-unit increase in CPH leads to a 0.523 increase in Cybersecurity Culture, supported by a significant t-statistic of 0.101 (p < 0.001). Similarly, Security Policy (SCP) demonstrates a positive relationship with CSC, with a one-unit increase resulting in a 0.041 increase in Cybersecurity Culture, supported by a significant t-statistic of 0.279 (p = 0.011). Training Completion Rate (TCR) also shows a statistically significant effect on CSC, with a one-unit increase associated with a 0.188 increase in Cybersecurity Culture, supported by a significant t-statistic of 1.139 (p < 0.001). Risk Awareness and Management (RKM) exhibits a positive effect on CSC, with a one-unit increase leading to a 0.239 increase in Cybersecurity Culture, supported by a significant t-statistic of 1.453 (p = 0.041). However, Behavioral Analytics (BHA) does not demonstrate a statistically significant effect on Cybersecurity Culture, as its coefficient estimate has a non-significant t-statistic.

The adjusted R-squared value for Model 3 is 0.831, indicating that the included independent variables explain approximately 83.1% of the variability in Cybersecurity Culture. Furthermore, the F-statistic of 16.144 (p < 0.000) suggests that the combined effects of the independent variables are statistically significant in explaining Cybersecurity Culture.

Based on the significance of the F-statistic and the rejection of the null hypothesis, it can be concluded that Security Awareness Programs and Behavioral Patterns significantly affect Cybersecurity Culture in Nigeria's deposit money banks.

Discussion of Findings

The descriptive findings reveal patterns within the socio-demographic characteristics of the surveyed population. In terms of educational background, a majority hold NCE/OND/HND qualifications (53.09%), followed by Bachelor's degrees (28.37%), and Master's degrees (18.54%). Age distribution showcases a significant portion within the 27 – 34 years bracket (52.53%), with presence in the 20 – 26 years range (18.82%). When considering years of experience, a significant portion falls within the 5 – 10 years category (46.07%), followed by those with less than 5 years (27.53%) and 11 – 15 years (23.87%). Interestingly, individuals with over 15 years of experience constitute a smaller segment (2.53%). Correlation and multicollinearity test highlight a lack of significant concerns, with variance inflation factor (VIF) values below 10 and tolerance levels exceeding 0.420. positive correlations among various variables indicate potential relationships worthy of further exploration.

The finding from the first hypothesis that Security Awareness Programs and Behavioral Patterns significantly affect Employee Feedback and Engagement is supported by scholars. Alghamdi (2021) used a quantitative research design, employing a survey questionnaire distributed to 415 respondents in Saudi Arabia. The data gathered through this method were then analyzed using Structural Equation Modeling (SEM) techniques, including path assessment and Confirmatory Factor Analysis (CFA). By investigating the relationship between cybersecurity awareness and employee behavior, the study identified significant effects of perceived barriers and security self-efficacy on employee behavior, thereby highlighting the crucial role of security awareness initiatives in influencing employee actions. In contrast, Lebek et al. (2013) conducted a literature review focusing on employees' information security awareness and behavior over the past decade. Through a comprehensive analysis of 113 publications, the review identified and categorized 54 theories in this field. By highlighting the critical role of employees as the weakest link in information security, the review emphasized the necessity for effective awareness programs and behavioral interventions. This aligns with the finding from the hypothesis by underlining the importance of such initiatives in enhancing employee engagement and influencing their feedback. Bhakuni and Saxena (2023) employed secondary qualitative methods, utilizing a systematic review approach to analyze their data. Their study explored the link between training and development, employee engagement, and retention. Their findings emphasized the positive impact of training on employee engagement, suggesting that investing in employees' skill development can lead to higher levels of engagement. This supports this finding by indicating that factors such as compliance adherence and training completion rate positively influence employee feedback and engagement.

The conclusion of the second hypothesis that Security Awareness Programs and Behavioral Patterns significantly affect Incident Response Time is supported by various studies. Stephanou and Dagada's (2008) ongoing study aim to evaluate the impact of information security awareness training on employees' security behavior. Although their research is still in progress, it emphasizes the crucial role of awareness initiatives in shaping on-the-job behavior, which directly correlates with incident response time. By focusing on understanding the influence of training on employees' security behavior, this study addresses a fundamental aspect of incident response effectiveness. Albrechtsen and Hovden's (2010) intervention study emphasized the importance of proactive engagement and dialogue in improving employee security behaviors. Their findings demonstrated significant changes in awareness and behavior indicators, suggesting that interventions focused on participation and collective reflection can lead to quicker incident response. This highlights the practical relevance of Security Awareness Programs in enhancing incident response time by fostering a security-conscious organizational culture. Alhuwail et al. (2021) investigated the factors influencing cybersecurity practices among healthcare professionals. Their findings indicated that professionals with more work experience demonstrated higher compliance with cybersecurity practices, emphasizing the role of training and experience in incident response. The study suggested that tailoring training based on internet usage patterns could further enhance incident response effectiveness, underscoring the importance of targeted approaches in Security Awareness Programs. Alzubaidi's (2021) assessment of cybersecurity awareness in Saudi Arabia identified areas for improvement, particularly in individual practices. By highlighting gaps in awareness, such as the use of public Wi-Fi and lack of knowledge about phishing attacks, the study contributes to understanding how Security Awareness Programs can enhance incident response capabilities. This emphasizes the need for comprehensive awareness initiatives that address specific vulnerabilities to effectively improve overall incident response time.

The main hypothesis concluded that Security Awareness Programs and Behavioral Patterns significantly affect Cybersecurity Culture finds support in several of the provided literature references. The findings of Alghamdi (2021) suggest that effective awareness initiatives can influence employee behavior, thereby contributing to developing a strong cybersecurity culture. Lebek et al. (2013) discuss the critical role of employees in information security and the need for effective awareness initiatives. Their literature review highlights various theories used to understand employees' information security awareness and behavior, emphasizing the importance of targeted interventions in fostering a robust cybersecurity culture. Organizations can cultivate a culture that prioritizes cybersecurity by addressing behavioral factors, such as awareness and adherence to security policies. Bhakuni and Saxena (2023) explore the link between training, employee engagement, and organizational performance. Their findings suggest that investing in training and development initiatives can lead to higher employee engagement levels, contributing to a positive organizational culture. This supports the findings that factors like compliance adherence and training completion rate positively influence cybersecurity culture by promoting a culture of continuous learning and improvement.

CONCLUSION

In conclusion, this study examines the nexus between Security Awareness Programs, Behavioral Patterns, and Cybersecurity Culture within Nigeria's Deposit Money Banks. Through a comprehensive analysis of key variables such as Compliance Adherence, Security Policy Acknowledgements, Training Completion Rate, Risk Awareness and Management, Behavioral Analytics, Employee Feedback and Engagement, and Incident Response Time. The descriptive analysis provided valuable insights into the socio-demographic characteristics of the population, shedding light on educational backgrounds, age distributions, and years of experience among respondents. Correlation and multicollinearity tests elucidated the relationships between variables and confirmed the absence of significant multicollinearity issues, bolstering the reliability of the data. Compelling evidence was revealed from the Hypothesis testing of the impact of Security Awareness

Programs and Behavioral Patterns on Employee Feedback and Engagement, Incident Response Time, and Cybersecurity Culture within Nigerian deposit money banks. Compliance Adherence, Training Completion Rate, and Risk Awareness and Management emerged as significant factors influencing Employee Feedback and Engagement, highlighting the importance of comprehensive security training initiatives. Also, Compliance Adherence, Security Policy Acknowledgements, Training Completion Rate, and Risk Awareness and Management were found to significantly affect Incident Response Time, highlighting the critical role of proactive security measures in mitigating cybersecurity incidents. Compliance Adherence, Security Policy Acknowledgements, Training Completion Rate, and Risk Awareness and Management were significant contributors to Cybersecurity Culture, emphasizing the necessity of fostering a security-conscious organizational culture. These findings have significant implications for stakeholders, including policymakers, bank management, cybersecurity professionals, and employees. The deep understanding of the relationship between Security Awareness Programs, Behavioral Patterns, and Cybersecurity Culture presented would inform the development of more effective cybersecurity strategies and risk management policies, ultimately enhancing the resilience of Nigerian deposit money banks against cyber threats.

REFERENCES

1. Adeloye, F. C. (2024). Claims Management and Performance of Insurance in Nigerian Manufacturing companies. *International Journal of Social Sciences Arts and Humanities, 11*(1), 13 – 24.
2. Akintoye, R., Ogunode, O., Ajayi, M., & Ambibola, A. J. (2022). Cyber security and financial innovation of selected deposit money banks in Nigeria. *Universal Journal of Accounting and Finance, 10*(3), 643-652. DOI:10.13189/ujaf.2022.100302.
3. Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security, 29*(4), 432-445. DOI: 10.1016/j.cose.2009.12.005
4. Alghamdi, Mohammed I. (2021). WITHDRAWN: Determining the impact of cyber security awareness on employee behaviour: A case of Saudi Arabia. DOI: 10.1016/j.matpr.2021.04.093
5. Alhuwail, D., Al-Jafar, E., Abdulsalam, Y., & AlDuaij, S. (2021). Information Security Awareness and Behaviors of Health Care Professionals at Public Health Care Facilities. *Applied Clinical Informatics, 12*(4), 924–932. DOI: 10.1055/s-0041-1735527
6. Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon, 7*(1). DOI: 10.1016/j.heliyon.2021.e06016
7. Andronache, A. (2021). INCREASING SECURITY AWARENESS THROUGH LENSES OF CYBERSECURITY CULTURE. *Journal of Information Systems & Operations Management, 15*(1).
8. Bhakuni, S., & Saxena, S. (2023). Exploring the link between training and development, employee engagement and employee retention. *Journal of Business and Management Studies, 5*(1), 173-180. DOI: 10.32996/jbms.2023.5.1.17
9. de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly, 34*(1), 1-7. https://doi.org/10.1016/j.giq.2017.02.007
10. Financier Worldwide Magazine. (2014). Financier Worldwide. Financier Worldwide. https://www.financierworldwide.com/banking-system-faces-cyber-threat
11. Fatoki, J. O. (2023). The influence of cyber security on financial fraud in the Nigerian banking industry. *International Journal of Science and Research Archive, 9*(2), 503-515. Article DOI: https://doi.org/10.30574/ijsra.2023.9.2.0609.
12. Hammarstrand, J., & Fu, T. (2015). Information security awareness and behaviour: of trained and untrained home users in Sweden.
13. Jean-Pierre, J. J. (2021). User Awareness and Knowledge of Cybersecurity and the Impact of training in the Commonwealth of Dominica (Doctoral dissertation, Walden University).
14. Jeanne Gobat. (2017, June 15). Banks: At the Heart of the Matter. *IMF.* https://www.imf.org/en/Publications/fandd/issues/Series/Back-to-Basics/Banks.

15. Kinley, D. (2017, March 1). Artful Dodgers: Banks and their Human Rights Responsibilities.
16. Krishnan, S. G., Al-Nahari, A., Ismail, N. A., & Yao, D. N. L. (2023). Enhancing Cybersecurity Awareness among Banking Employees in Malaysia: Strategies, Implications, and Research Insights. *International Journal of Academic Research in Business and Social Sciences, 13*(8), 643–660. http://dx.doi.org/10.6007/IJARBSS/v13-i8/17413.
17. Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., & Hohler, B. (2013, January). Employees' information security awareness and behavior: A literature review. In 2013 46th Hawaii International Conference on System Sciences (pp. 2978-2987). IEEE. DOI: 10.1109/HICSS.2013.192
18. Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., et al. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecur, 3*(10). https://doi.org/10.1186/s42400-020-00050-w
19. Mariah St. John. (2024, April 17). Cybersecurity Stats: Facts And Figures You Should Know. *Forbes*. https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/#Sources
20. Narayanan, L. (2024, May 6). Benefits and Importance of Cybersecurity in Banking Sector. *Teceze*. https://teceze.com/cybersecurity-in-banking-importance-and-threats-challenges-benefits
21. Ojeka, S. A., & Egbide, B. C. (2017). Cyber security in the Nigerian banking sector: an appraisal of audit committee effectiveness. *International Review of Management and Marketing, 7*(2), 340-346.
22. Okolo, F. (2023). Cargo Security Examination and it's effect on National Security in the United State. *IJARIIE*, 9(1), 1380 – 1388.
23. Stephanou, T., & Dagada, R. (2008, July). The Impact of Information Security Awareness Training on Information Security Behaviour: The Case for Further Research. In ISSA (pp. 1-21).
24. Statista. (2024). Banking – Worldwide | Statista Market Forecast. *Statista.* https://www.statista.com/outlook/fmo/banking/worldwide.
25. Sasu, D. D. (2022). Topic: Banking industry in Nigeria. *Statista.* https://www.statista.com/topics/9747/banking-industry-in-nigeria/#topicOverview.
26. 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), 387-396. DOI:10.12785/ijcds/080407.