http://journals.uonbi.ac.ke/index.php/adfj
ISSN 2522-3186

African Development Finance Journal http://journals.uonbi.ac.ke/index.php/adfj
November Vol 8 No.9, 2025 PP 276-299 ISSN 2522-3186

Unmasking the Path to Sustainable Fraud Mitigation through Cybersecurity Investments: Insights from Commercial Banks in Tanzania

By: Justus Gratian Mwemezi [1] and Amos Abnery Nzaga [2]

Abstract

This study investigates how cybersecurity investments contribute to sustainable fraud mitigation in Tanzanian commercial banks. Using quantitative research design, data were collected from 293 banking professionals across ten banks, including IT, risk, compliance, and cybersecurity officers. Analysis using SmartPLS revealed that Incident Response Preparedness, Fraud Detection Systems Effectiveness, and Customer Awareness Programs significantly enhance fraud mitigation, while technological investments, employee training, and cybersecurity culture showed no significant impact. The model explained 53.2% of the variance in fraud mitigation outcomes, indicating strong explanatory power. The findings emphasize that banks should prioritize capability-based measures—such as detection systems and response readiness—over mere capital expenditure. Policymakers and regulators are encouraged to integrate cybersecurity into governance frameworks for long-term sustainability. The study provides novel empirical evidence from Tanzania, advancing understanding of how capability-driven cybersecurity strategies enhance fraud resilience in emerging financial markets.

Keywords: *Cybersecurity investments, Fraud mitigation, Sustainable banking, Tanzanian commercial banks.*

1. Introduction

The rapid advancement of digital technologies has significantly reshaped the global banking landscape, presenting both opportunities and challenges for financial institutions (Cele & Kwenda, 2025). Artificial intelligence (AI) is transforming the cybercrime landscape at an unmatched speed. Technology integration has enhanced convenience, expanded financial inclusion, and allowed broader access to financial services, especially in underserved regions. Across the globe, financial institutions are now facing an unprecedented surge in digital fraud, fueled by AI-enabled attacks, sophisticated phishing campaigns and increasingly bold cybercriminal networks. A 2024 annual report by Huntington Bank highlights a 1,265% rise in phishing emails worldwide (World Bank, 2022), while Visa's 2023 cybersecurity initiatives successfully blocked 80 million fraudulent transactions worth $40 billion globally (Reuters, 2023). Additionally, the Wall Street Journal reported that financial institutions globally are projected to spend approximately $230 billion on

[1] *The Institute of Finance Management (IFM)Tanzania, E-Mail: jmwemezitz@gmail.com*
[2] *Exim Bank (Tanzania) Limited, E-Mail: nzagajunior@gmail.com*

compliance and fraud prevention in 2024, reflecting a recognition of the critical need for robust cybersecurity measures (Cele & Kwenda, 2025).

In Africa, the situation is particularly acute. According to Interpol's *African Cyberthreat Assessment Report* (2024), ransomware attacks and phishing schemes targeting African banks have surged by over 200% in three years, with Tanzania ranked among the most vulnerable (Interpol, 2024). Despite notable investments in cybersecurity technologies, fraud continues to bypass even sophisticated controls, raising a critical question: Are these cybersecurity investments sustainable in preventing fraud, or are they merely reactive responses to an evolving threat landscape? Studies in East Africa further emphasize that phishing and social engineering remain dominant tactics cybercriminals use, exposing the need for stronger customer education and improved internal controls (Mwita & Mhina, 2023; Serianu, 2023). Moreover, while cybersecurity spending increases, governance gaps remain a significant obstacle. Only 22% of East African financial institutions actively involve their boards in cybersecurity oversight, reflecting a strategic disconnect between operational security measures and executive decision-making (The East African, 2024).

In Tanzania, commercial banks have responded by increasing cybersecurity budgets and implementing cybercrime mitigation strategies centered around public awareness campaigns, management support, technology acquisition, and employee training (Mwita & Mhina, 2023). However, persistent cyberattacks highlight systemic weaknesses, including limited digital literacy, inadequate technological infrastructure, and fragmented regulatory enforcement (Thati *et al.*, 2025). Deloitte (2023) reports that banks allocate less than 5% of their operational budgets to cybersecurity, significantly below the global benchmark of 10–15%, suggesting underinvestment in critical risk areas.

The global research affirms that planned cybersecurity investments, especially those incorporating AI, blockchain, machine learning, and biometrics, can effectively mitigate fraud (Alex-Omiogbemi *et al.*, 2024b). For instance, the South African banking sector has successfully leveraged advanced technologies such as filtering software, data mining, and firewalls to combat cybercrime (Akinbowale, Mashigo & Zerihun, 2023). These success stories emphasize the

importance of adopting a multi-dimensional cybersecurity strategy that blends technology with human capacity development and robust governance frameworks. However, despite the growing body of global and regional research, there remains a significant gap. Most studies narrowly focus either on the technical aspects of cybersecurity or short-term cost-benefit analyses. Very few explore whether cybersecurity investments foster sustained fraud mitigation particularly in emerging economies like Tanzania, where challenges like low digital literacy, regulatory fragmentation, and resource constraints create unique dynamics (Kayumbe and Gilliard, 2024; Semlambo and Shalua, 2024). Moreover, research often overlooks the interconnected roles of organizational culture, employee readiness, customer awareness programs, and governance practices in shaping the long-term effectiveness of cybersecurity strategies.

This study makes three key contributions**.** First, it extends the discourse on fraud prevention by integrating sustainability into the evaluation of cybersecurity investments, moving beyond short-term loss reduction to long-term resilience, an angle rarely addressed in the literature (Saini & Sahu, 2024). Second, it brings fresh empirical evidence from the Tanzanian banking sector, an underexplored context in global cyber fraud research (Deloitte, 2023), thereby providing insights that challenge and enrich existing theories predominantly built on developed-economy data. Third, this study advances the Protection Motivation Theory into sustainable cyber resilience by adopting a multi-dimensional model that includes factors that capture technological, organizational, and human-capital elements (Prentice-Dunn & Rogers, 1986). The urgency of this investigation is heightened by the rapid escalation of AI-enabled cyber fraud, which has grown in phishing-related attacks in recent years, raising the stakes for banks to adopt adaptive, future-proof strategies. In doing so, this study addresses a pressing policy and operational challenge in emerging markets and offers methodological and theoretical innovations relevant to scholars, practitioners, and regulators seeking to future-proof financial institutions against evolving cyber threats.

1.2 Research Problem

Effective cybersecurity measures in the banking sector should safeguard financial institutions from fraud, protect customer data, and maintain trust in financial systems. This requires strong governance, adequate budgetary allocations, advanced technological defenses, and regular audits aligned with international standards (Thati et al. 2025). Despite substantial investments in

cybersecurity infrastructure, Tanzanian commercial banks continue to experience escalating incidents of cyber fraud. Between September and December 2023, losses from mobile and internet banking fraud rose by 84%, while ATM card skimming increased by 60% (Bank of Tanzania, 2024).

Existing research in Tanzania and Sub-Saharan Africa remains fragmented, with most studies focusing on isolated components such as technical controls, employee training, or customer awareness, without assessing how these elements interact to produce long-term resilience. Weak identity verification systems further exacerbate fraud risks, with over 80% of identity fraud incidents in Africa linked to misuse of national identity documents (PwC Tanzania, 2025). These challenges undermine customer trust, erode the financial stability of banks, and expose the broader financial system to systemic risks. Rising cyber fraud incidents not only increase operational losses and non-performing loans but also slow down digital banking adoption, limiting Tanzania's efforts to build a resilient, technology-driven financial sector (Nyamwihula, 2024).

Moreover, there is limited empirical evidence examining the effectiveness of cybersecurity investments within the specific institutional, regulatory, and socio-economic contexts of developing economies. Key questions remain unanswered: Which dimensions of cybersecurity investments contribute to sustainable fraud mitigation? Do technological expenditures matter more than organizational preparedness or customer awareness? This study seeks to provide actionable recommendations to strengthen governance frameworks, optimize cybersecurity investments, and enhance fraud prevention.

1.3 Research Objectives

The study sought to address the following research objectives:

1. To evaluate the effect of organizational cybersecurity capabilities on sustainable fraud mitigation in Tanzanian commercial banks.
2. To assess the influence of operational readiness factors on banks' ability to mitigate cyber fraud.
3. To examine the role of customer-focused cybersecurity initiatives in enhancing sustainable fraud mitigation outcomes.

2.0 Literature Review

2.1 Theoretical background and research framework

According to Tariq *et al.* (2024) and Li *et al.* (2022), cybersecurity is a multidisciplinary field that integrates concepts from other fields, including computer science, cryptography, information security, risk management, and human behaviour. Cybersecurity has become a defining capability in modern banking, with studies highlighting its dual role in preventing fraud and maintaining trust in digital services. Globally, investments in advanced fraud detection systems leveraging artificial intelligence, blockchain, and biometrics have been shown to significantly reduce fraud incidents (Alex-Omiogbemi *et al.*, 2024a).

Research in emerging markets reveals advancements and persistent challenges in combating cyber fraud. Conversely, banks face systemic barriers, including low digital literacy, limited cybersecurity budgets, and fragmented regulations, which undermine the effectiveness of such investments (Deloitte, 2023). Studies in Uganda and Kenya highlight governance gaps and underinvestment in human capital as key drivers of vulnerability (Serianu, 2023). In Tanzania, existing literature is limited and fragmented, focusing on technical fraud detection systems (Pallangyo, 2022) and awareness initiatives (Mwita and Mhina, 2023), with few adopting a sustainability perspective that integrates technology, employee readiness, organizational culture, and customer awareness. Addressing this gap aligns with global calls to position cybersecurity not merely as a cost center, but as a strategic enabler of long-term resilience.

This study is underpinned by Protection Motivation Theory (PMT), initially developed by Rogers (1986) and widely applied in health psychology, organizational behavior, and more recently, in cybersecurity research (Haag, Siponen & Liu, 2021; Khan *et al.*, 2022; Siponen *et al.*, 2024). PMT explains how individuals and organizations are motivated to adopt protective behaviors in response to perceived threats. In the context of this study, PMT helps explain how Tanzanian commercial banks respond to increasing cyber fraud by evaluating both the threats (rising fraud incidents, digital vulnerabilities) and coping strategies (investing in technology, employee training, and customer awareness).

Importantly, PMT allows for the inclusion of both technological and human behavioral dimensions, making it particularly suitable for analyzing sustainable fraud mitigation in banks. Recent cybersecurity studies have used PMT to investigate how threat perceptions and coping capabilities influence decisions related to IT security adoption, fraud prevention strategies, and policy compliance (e.g., Wang, Y., Zhang, Y., Chang, X., and Kang, 2024).. Based on the theoretical foundation and reviewed literature, the research framework for this study proposes that six independent variables each representing a key area of cybersecurity investment, influence the dependent variable, sustainable cyber fraud mitigation in banks, as indicated in Figure 1.

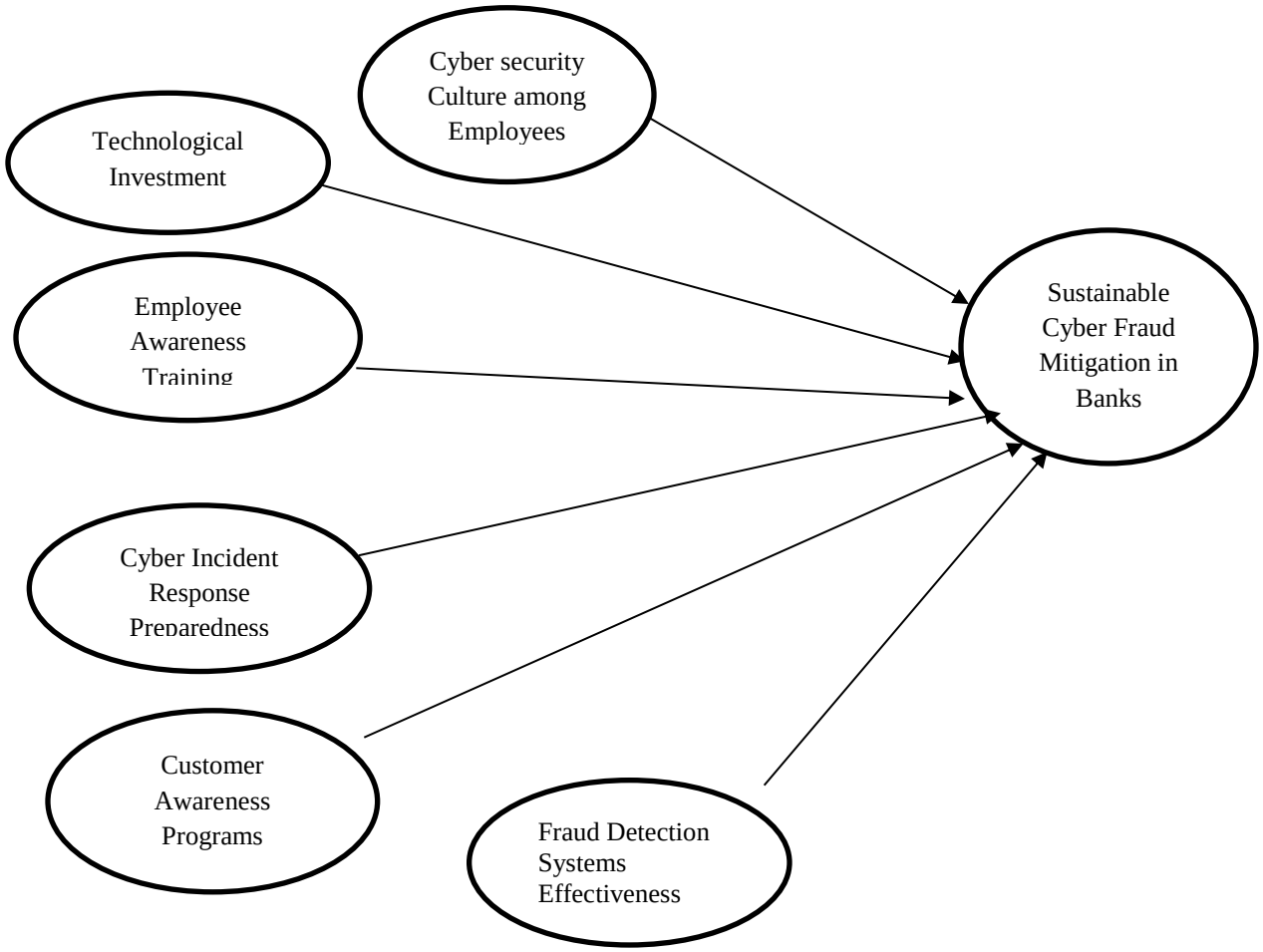

Figure 1: Conceptual model

2.2 Technological Investment

Studies in Nigeria and South Africa have highlighted the correlation between cyber risks and investment decisions, emphasizing the need for effective mitigation strategies (Ebenezer, Paula, & Allo, 2016). The South African banking industry employs various anti-fraud technologies, including filtering software, firewalls, and data mining, positively affecting cyber fraud mitigation (Akinbowale, Mashigo & Zerihun, 2023). Key strategies to combat evolving threats like phishing and malware attacks include implementing advanced authentication mechanisms, investing in fraud detection systems, and promoting cybersecurity awareness (Mehta, 2021). Recommendations for mitigating cyber fraud include developing citizen-friendly policies, investing in emerging technologies, and enhancing human capacities to effectively deploy these technologies (Jegede et al., 2016; Akinbowale et al, 2024). Thus, the following hypothesis is proposed:

H_1: A significant positive relationship exists between technological investment and cyber fraud mitigation in Tanzanian commercial banks.

2.3 Employee Awareness Training

Research indicates that comprehensive training programs significantly reduce the likelihood of phishing attacks and strengthen overall cyber defences (Basir *et al.*, 2024). Practical training empowers employees to recognize and respond to cyber threats, making them the first line of defence against attacks (Tolossa, 2023). However, traditional training methods often fall short, being perceived as dull and ineffective in addressing the rapidly evolving cybersecurity landscape (Almehdhar *et al.*, 2024). To maximize impact, organizations should implement ongoing, tailored training programs that combine thorough education, advanced technology, and proactive risk management strategies (Tolossa, 2023; Basir *et al.*, 2024). This approach fosters a culture of cybersecurity consciousness and enhances an organization's resilience against cyber threats. Consequently, the following hypothesis is put forth:

*H_2**:** Employee awareness training has a significant positive effect on cyber fraud mitigation*

2.4 Cyber Incident Response Preparedness

Studies emphasize the need for comprehensive frameworks that combine machine learning, early warning systems, and proactive mitigation models (McAnyana et.al, 2020; Chhabra Roy, 2024). These approaches enable efficient prioritization of cyber fraud and enhance resilience to cyber threats. A grounded theory study proposes an e-commerce fraud incident response framework, defining processes, roles, and stakeholders (Dwight, 2024). To improve incident response effectiveness, organizations should adopt structured playbooks, enhance cross-team collaboration, and prioritize communication (Ismail, 2024). A shift from reactive to proactive mitigation approaches is crucial for sustainable cyber fraud prevention and response in an increasingly complex threat landscape. Therefore, this study postulates that:

> *H_3: Cyber incident response preparedness significantly contributes to effective cyber fraud mitigation.*

2.5 Cybersecurity Culture among Employees

A strong cybersecurity culture, fostered through training programs, leadership support, and employee engagement, is essential for effective cybercrime prevention (Da Veiga *et al.*, 2020; De Silva, 2023). Empirical research has shown that policy factors, employee behavior, and cybersecurity awareness significantly impact the effectiveness of cybersecurity measures in IT organizations (Thati *et al.*, 2025). The human factor is critical, as even advanced security technologies cannot protect an organization if employees make poor decisions that expose systems to attackers (Lie, Utomo & Winarno, 2021). Leaders must invest in security technologies and practical solutions to address human errors in cybersecurity. Ultimately, a robust cybersecurity culture encourages all employees to act positively in reducing organizational risks from cyberattacks. Therefore, this study hypothesizes that:

> *H_4: A strong cybersecurity culture among employees is positively associated with sustainable cyber fraud mitigation.*

2.6 Fraud Detection Systems Effectiveness

Fraud Detection Systems (FDS) are crucial in mitigating cyber fraud in the banking sector. Studies have shown that combining internal and external anti-fraud technologies, including filtering software, firewalls, and data mining, can positively impact cyber fraud mitigation (Akinbowale

et.al, 2023). The effectiveness of FDS is enhanced by integrating advanced technologies such as machine learning, artificial intelligence, and blockchain (Soni *et al.*, 2022). A comprehensive framework incorporating machine learning, early warning signs, and proactive mitigation models has been proposed to address gaps in existing cybersecurity systems (Roy *et al.*, 2024). Research has demonstrated that AI-based software, notably the Random Forest algorithm, can achieve real-time fraud detection with high accuracy rates of up to 83.94% (Rojan, 2024). Based on the literature, this study postulates that:

H_5: The effectiveness of fraud detection systems is positively associated with cyber fraud mitigation outcomes

2.7 Customer Awareness Programs

Customer awareness programs are crucial in mitigating cyber fraud in the banking sector. Social engineering remains a predominant technique cybercriminals use to exploit human vulnerabilities (Tariq *et al.*, 2024). Practical training and education programs can significantly increase user awareness and reduce cybersecurity incidents (Mwita & Mhina, 2023). However, organizations still face challenges in developing human knowledge to protect against social engineering attacks, with factors such as business environment and social and personal aspects influencing users' proficiency in threat detection (Aldawood & Skinner, 2019). To address these issues, banks should implement targeted awareness initiatives, increase community engagement, and utilize local media for awareness campaigns, focusing on vulnerable groups to ensure comprehensive cybersecurity knowledge among customers (Gueorgiev *et al.*, 2025). As a result, this study postulates that:

H_6: Customer awareness programs have a significant positive influence on the mitigation of cyber fraud.

3.0 Research Methodology

3.1 Research Design, Population

This study employed a quantitative, cross-sectional research design to investigate the influence of cybersecurity investments on sustainable fraud mitigation in Tanzanian commercial banks. This design enables the assessment of relationships among predefined variables using standardized data across multiple institutions simultaneously. The study targeted key cybersecurity and fraud prevention employees, including Cybersecurity Officers, IT Specialists, Fraud Risk Officers, Compliance Officers, and Customer Relationship Officers. These individuals were selected for

their direct involvement in implementing, monitoring, and evaluating cybersecurity measures. The research focused on a defined population of 384 employees drawn from ten purposively selected commercial banks in Dar es salaam city, where the headquarters of all banks are centered. These banks were chosen to reflect diversity in operational scale, involving large and small banks and levels of digital service adoption. Together, they provide a representative view of the cybersecurity landscape in the Tanzanian banking sector.

3.2 Research Instrument Development

The study employed a **structured questionnaire** as the primary data collection instrument, designed to capture perceptions and experiences of bank employees regarding cybersecurity investments and fraud mitigation. The instrument was developed based on **validated measurement items** adapted from previous empirical studies, ensuring **content validity** and **contextual relevance.** Items were aligned with the constructs identified in the conceptual framework. Each construct was measured using **more than four items** on a **5-point Likert scale** (1 = Strongly Disagree to 5 = Strongly Agree). Sources of the items were documented to maintain academic rigour and traceability. A **pilot test** involving 12 respondents from two banks assessed the questionnaire's clarity, reliability, and relevance. Minor wording adjustments were made based on feedback, and **Cronbach's alpha** results confirmed satisfactory internal consistency ($\alpha > 0.70$ for all constructs).

3.3 Sampling and Data Collection

To determine the minimum required sample size from the population of 384 cybersecurity-related employees across the selected banks, Yamane's (1967) formula was applied with a 5% margin of error. **Yamane's (1967) formula** was selected for its simplicity, reliability, and suitability when determining sample size from a known, finite population. The study employed a stratified random sampling technique, where banks were first grouped by size (large and small) to ensure proportional representation. Within each bank, simple random sampling was used to select respondents holding relevant roles. Data were collected using a self-administered structured questionnaire, distributed physically and electronically to respondents. Before full deployment, a pilot test was conducted with 12 participants to refine the instrument for clarity and reliability. Data collection spanned four weeks, with follow-ups to maximize response rates while maintaining

voluntary participation and confidentiality. Out of 388 respondents who received the questionnaire, 303 submitted their responses. However, after screening the data set, 293 questionnaires were considered complete and valid for subsequent data analysis. The profiles of the participants who represented their banks are shown in Table 1.

Since the data were collected from a single source using self-reported questionnaires, there was a potential risk of common method bias (CMB), which can artificially inflate the observed relationships among constructs (Podsakoff, MacKenzie & Podsakoff, 2012). To assess this risk, variance inflation factors (VIFs) were examined, as Kock (2015) recommended, who suggests that CMB is unlikely to be a serious issue if all VIF values are below the threshold of 3.3. As presented in Table 2, all computed VIFs fall well below this cutoff, indicating that multicollinearity is not a concern and that the results are not significantly affected by common method variance (Diamantopoulos, Riefler & Roth, 2008; Kock, 2015).

4.0 Data Analysis

4.1 Respondent Demographics

The study drew responses from a well-qualified and experienced group of banking professionals. In Table 1, a majority **(63.8%)** held undergraduate-level qualifications, while **33.9%** had postgraduate degrees, reflecting a high level of academic preparedness relevant to cybersecurity and fraud mitigation. Key roles represented included **compliance officers and customer relationships officers, IT managers, risk officers,** and **cybersecurity officers,** ensuring broad functional coverage of operational, compliance, and technical perspectives. Regarding work experience, over **55% had between 4 and 10 years,** and **21.8% had more than 10 years**, indicating strong institutional knowledge and insight. Additionally, **73.8% of respondents had received cybersecurity training,** underscoring the sector's ongoing efforts to build cyber resilience across professional roles.

Table 1: Summary of Respondent Demographics (N = 293)

Variable	Category	Frequency (n)	Percentage (%)
Education Level	Undergraduate (Diploma + Bachelor)	187	63.8%
	Postgraduate (Master + PhD)	99	33.9%
	Others	7	2.3%
Job Title	IT Manager	50	16.9%
	Cybersecurity Officer	37	12.6%
	Risk Officer	45	15.3%
	Customer Relationship Officer	62	21.3%
	Compliance Officer	64	21.9%
Work Experience	Less than 3 years	67	22.9%
	4–10 years	162	55.3%
	Over 10 years	64	21.8%
Cybersecurity Training	Yes	216	73.8%
	No	77	26.2%

4.2 Data Analysis Techniques

The study's conceptual framework was evaluated using partial least squares structural equation modelling (PLS-SEM). Because this study is prediction-oriented, PLS-SEM is a better statistical technique to examine the theoretical model than a different approach like covariance-based modelling(Hair, Sarstedt & Ringle, 2019; Mwemezi & Mandari, 2024). Data analysis was conducted using SmartPLS software version 3. The study assessed the measurement model to ensure it was valid and reliable before analyzing the structural model using the bootstrapping approach.

5.0 Results of the Study

5.1 Assessment of the Measurement Model

It was important to evaluate the measurement model for internal reliability, convergent validity, and discriminant validity (Hair *et al.*, 2021). Factor loadings, composite reliability (CR), and average variance extracted (AVE) were examined to assess convergent validity. According to Hair *et al.* (2017), acceptable thresholds are factor loadings above 0.7, AVE above 0.5, and CR above 0.7 for establishing convergent validity, discriminant validity, and internal reliability. The results of this study revealed that all factor loadings met the recommended minimum of 0.7 (refer to Table 2), except for two items under technological investment (TI4) and employee awareness training

(ET3), which were removed. Additionally, all constructs' AVE and CR values fell within the acceptable range of 0.5 and 0.7, confirming that the model achieved convergent validity.

Table 2. Reliability and validity of the measurement model

Construct	Item	Factor Loading	VIF	CR	AVE
Technological Investment	TI1	0.785	1.116	0.930	0.688
	TI2	0.847	1.095		
	TI3	0.836	2.944		
	TI5	0.815	2.563		
	TI6	0.860	1.142		
	TI7	0.832	2.581		
Employee Awareness Training	ET1	0.784	2.411	0.924	0.671
	ET2	0.818	2.345		
	ET4	0.789	1.967		
	ET5	0.884	1.705		
	ET6	0.790	2.223		
	ET7	0.845	2.489		
Cyber Incident Response Preparedness	IRP1	0.804	1.375	0.939	0.720
	IRP2	0.863	2.780		
	IRP3	0.793	2.193		
	IRP4	0.901	1.672		
	IRP5	0.892	1.773		
	IRP6	0.834	2.496		
Customer Awareness Programs	CA1	0.893	1.830	0.954	0.774
	CA2	0.856	2.200		
	CA3	0.907	2.754		
	CA4	0.919	2.189		
	CA5	0.852	1.515		
	CA6	0.851	1.967		
Cyber security Culture among Employees	CC1	0.863	2.897	0.936	0.744
	CC2	0.884	2.414		
	CC3	0.886	1.503		
	CC4	0.829	2.126		
	CC5	0.852	2.476		
Fraud Detection Systems Effectiveness	FD1	0.838	1.314	0.922	0.665
	FD2	0.852	1.460		
	FD3	0.846	2.236		
	FD4	0.858	1.176		
	FD5	0.848	2.774		
Sustainable Cyber Fraud Mitigation in Banks	FM1	0.903	1.390	0.925	0.756
	FM2	0.875	1.123		
	FM3	0.875	2.348		
	FM4	0.822	1.984		

The discriminant validity was assessed using the Heterotrait–Monotrait (HTMT) ratio criterion (Henseler, Ringle, & Sarstedt, 2015). As presented in Table 3, all HTMT values were below the recommended cutoff of 0.85 (Kline, 2016). This confirms that the data satisfied the requirements for discriminant validity.

Table 3. Discriminant validity (HTMT)

	CA	CC	FD	FM	TI	ET	IRP
Awareness							
Culture	0.668						
Detection	0.743	0.827					
Mitigation	0.691	0.603	0.727				
Tech Investment	0.652	0.622	0.682	0.538			
Training	0.770	0.792	0.743	0.659	0.819		
preparedness	0.720	0.807	0.783	0.676	0.729	0.828	

5.2 Assessment of the Structural Model

The structural model was evaluated to examine the hypothesized relationships between the study constructs. The model explained **53.2%** of the variance in FM (R^2 = 0.532), indicating moderate explanatory power (Cohen, 1988). The predictive relevance assessment showed that the **Q^2** value was above zero, confirming that the model possesses predictive capability (Shmueli *et al.*, 2019). Effect size analysis revealed that all f^2 values fell between **0.019 and 0.096**, representing small to medium effects (Cohen, 1988).

Table 4. Hypotheses Testing

Hypotheses	Relationships	Original Sample (O)	t-values	p-values	Remarks
H1	TI -> FM	-0.064	0.977	0.328	Not supported
H2	ET -> FM	0.134	1.429	0.153	Not supported
H3	IRP -> FM	0.198	3.066	0.002	Supported
H4	CC -> FM	-0.081	1.052	0.293	Not supported
H5	FD -> FM	0.367	4.318	0.000	Supported
H6	CA -> FM	0.250	3.668	0.000	Supported

Carrying out a bias-corrected and accelerated (BCA) bootstrapping technique with 5,000 resamples, the results in **Table 4** indicate that three of the six proposed hypotheses were statistically supported at 95% confidence intervals. Specifically, **Incident Response Preparedness (IRP)** had a positive and significant effect on **Fraud Mitigation (FM)** ($\beta = 0.198$, $t = 3.066$, $p = 0.002$), **Fraud Detection Systems Effectiveness (FD)** exhibited a strong positive and significant effect ($\beta = 0.367$, $t = 4.318$, $p < 0.001$), and **Customer Awareness Programs (CA)** also demonstrated a significant positive influence ($\beta = 0.250$, $t = 3.668$, $p < 0.001$). In contrast, the

effects of **Technological Investment (TI)** (β = –0.064, *p* = 0.328), **Employee Training (ET)** (β = 0.134, *p* = 0.153), and **Cybersecurity Culture (CC)** (β = –0.081, *p* = 0.293) on FM were statistically non-significant.

6. Discussion of Results, Theoretical and Practical Implications

6.1 Discussion of Results

This study assessed the role of six dimensions of cybersecurity investments: Technological Investment (TI), Employee Training (ET), Incident Response Preparedness (IRP), Cybersecurity Culture (CC), Fraud Detection Systems Effectiveness (FD), and Customer Awareness Programs (CA)—in promoting sustainable fraud mitigation (FM) in Tanzanian commercial banks. The findings reveal that only IRP, FD, and CA have statistically significant positive effects, underscoring the multi-dimensional nature of fraud prevention in banking systems, especially within developing economies.

In contrast to the prior hypothesis (H1), the relationship between TI and fraud mitigation was negative and statistically non-significant (β = –0.064, *p* = 0.328), suggesting that increased technological spending alone does not necessarily reduce fraud incidents. This finding echoes Karanja and Rosso (2017) argument that technology without corresponding human, procedural, and governance alignment often fails to deliver measurable security outcomes. In the Tanzanian context, this may reflect the implementation of technological tools without adequate integration into operational workflows or sufficient technical capacity to maximize utility (Deloitte, 2022).

Employee training had a positive but statistically nonsignificant relationship with FM (β = 0.134, *p* = 0.153). Although employee training is widely acknowledged as essential in mitigating cyber risks (Tolossa, 2023; Basir *et al.*, 2024), the current findings indicate that training programs in Tanzanian banks may lack adequate frequency, coverage, or alignment with evolving cyber threat landscapes. This aligns with regional observations that training initiatives in East African banks often remain reactive rather than anticipatory, limiting their long-term impact (Pallangyo, 2022).
H3 investigated how the incident response preparedness of commercial banks can mitigate cyber fraud. IRP emerged as a significant predictor of FM (β = 0.198, *p* = 0.002), reinforcing the value of structured and tested incident response protocols in containing cyber fraud. This finding aligns

with McAnyana et al. (2020), who emphasize that rapid response capabilities, clear escalation channels, and interdepartmental coordination can significantly reduce the impact of security breaches. Given Tanzania's documented increase in fraud incidents, these results suggest that proactive readiness plays a crucial role in fraud resilience.

Surprisingly, cybersecurity culture among employees was found to have a negative and non-significant influence on FM ($\beta = -0.081$, $p = 0.293$). While literature consistently identifies cybersecurity culture as a critical enabler of security outcomes (Da Veiga *et al.*, 2020; De Silva, 2023), this result indicates that such a culture may still be in its formative stages in Tanzanian banks. Cultural transformation in cybersecurity typically requires sustained leadership commitment, policy reinforcement, and continuous awareness programs before yielding tangible results (Aksoy, 2024).

Fraud detection systems' effectiveness showed the strongest positive and significant relationship with FM ($\beta = 0.367$, $p < 0.001$). This finding corroborates studies from South Africa and Nigeria, where advanced detection systems—incorporating AI, real-time analytics, and anomaly detection—have been linked to significant reductions in cyber fraud (Akinbowale et.al, 2024). In the Tanzanian context, this emphasizes the critical role of real-time detection capabilities in addressing traditional and emerging fraud schemes.

Customer awareness programmes also exhibited a significant positive influence on FM ($\beta = 0.250$, $p < 0.001$), supporting evidence from global studies that position customer education as a central component of sustainable fraud prevention (Mhina & Lashayo, 2024; Gueorgiev *et al.*, 2025). In regions with varying levels of digital literacy, such as Tanzania, awareness initiatives that educate customers about phishing, social engineering, and safe banking practices are particularly impactful (Pallangyo, 2022).

6.2 Theoretical and Practical Implications

This study advances theory by mirroring the **Protection Motivation Theory (PMT) (Rogers, 1986)** into the underexplored domain of organizational-level cybersecurity investments and fraud mitigation within developing economies. This study operationalizes the PMT constructs in the

banking sector of Tanzania, demonstrating the path to sustainable fraud mitigation through cybersecurity investments. The results challenge conventional assumptions that **technological investment and employee training automatically yield stronger fraud resilience (Victory et al., 2022; Tolossa, 2023; Alex-Omiogbemi *et al.*, 2024a)**. Instead, sustainable outcomes are driven by **incident response preparedness, fraud detection Systems, and customer awareness programs,** highlighting that the effectiveness of responses rather than the volume of inputs best explains fraud mitigation. This finding underscores the **socio-technical nature of cybersecurity**, shifting the debate from resource intensity to organizational readiness and customer engagement. Moreover, despite its prominence in prior studies (Da Veiga *et al.*, 2020; De Silva, 2023), the non-significance of cybersecurity culture suggests that cultural transformation is a **long-term process** requiring sustained reinforcement before measurable outcomes emerge (Aksoy, 2024).

The findings carry important implications for practitioners, policymakers, and regulators in the banking sector. First, the strong effects of **fraud detection systems and incident response preparedness** highlight that sustainable fraud mitigation depends less on budget size and more on the **strategic effectiveness of organizational capabilities**. Banks should prioritize advanced fraud analytics, AI-driven anomaly detection, and real-time monitoring (Rojan, 2024), while embedding structured playbooks, simulation exercises, and interdepartmental coordination to strengthen proactive readiness. This ensures that technology adoption is not isolated but fully integrated into operational workflows. Second, the significance of **customer awareness programs** underscores the need to extend cybersecurity beyond internal systems to external stakeholders. Given the persistent role of phishing and social engineering in developing economies (Serianu, 2023), banks should intensify digital literacy initiatives through multi-channel education campaigns, targeted outreach to vulnerable demographics, and collaborative programs with regulators and telecom operators. Such measures strengthen the human firewall, often the weakest link in cybersecurity. Third, the **non-significance of employee training and cybersecurity culture** raises critical managerial lessons. The results suggest that existing training may be too generic, compliance-oriented, or unevenly implemented. Banks must redesign training to be **role-specific, skills-based, and outcome-driven**, moving away from tick-box exercises (Mwita & Mhina, 2023). Similarly, the weak statistical effect of culture implies that transformation requires **long-term leadership commitment and institution-wide alignment,** rather than fragmented awareness efforts. Finally,

the study carries **policy implications**. Regulators must recognize that mandating higher cybersecurity expenditure is insufficient if investments are not tied to demonstrable outcomes. Instead, emphasis should be placed on **risk-based frameworks, periodic cyber incident drills, sector-wide knowledge-sharing, and measurable performance standards**. Such governance approaches harmonize practices across banks, build resilience at the ecosystem level, and ultimately strengthen public trust in the financial system.

7.0 Limitations and Future Research Directions

Although the study achieved its objectives, it was not without limitations, as is common in empirical research. This study offered theoretical and practical contributions by comprehensively analyzing the variables influencing banks to embrace sustainable fraud mitigation. However, using cross-sectional data poses a limitation, as the findings may vary over time. For instance, the outcomes may differ if banks take longer to embrace fraud mitigation measures. Therefore, a longitudinal research design could be considered in future studies to capture changes over time. Additionally, the constructs were measured perceptually, with the model yielding a coefficient of determination (R^2) of 53.2%, indicating that other unexplored factors may also influence the adoption of sustainable fraud mitigation. Future research could address this by incorporating multi-source data such as security logs, security operations center (SOC) metrics and customer complaint records to triangulate perceptions and enhance the robustness of the findings.

References

African, E. (2024) *Cyber security top concern for many East African firms*. Available at: https://www.theeastafrican.co.ke/tea/business-tech/cyber-security-top-concern-for-many-east-african-firms-4840530 (Accessed: 28 May 2025).

Akinbowale, O.E., Klingelhöfer, H.E. and Zerihun, M.F. (2024) 'Investigating the level of effectiveness of the anti-fraud technologies employed by the South African banking industry for cyberfraud mitigation', *Journal of Financial Crime*, 31(1), pp. 201–225.

Akinbowale, O.E., Mashigo, P. and Zerihun, M.F. (2023) 'The integration of forensic accounting and big data technology frameworks for internal fraud mitigation in the banking industry', *Cogent Business & Management*, 10(1), p. 2163560.

Aksoy, C. (2024) 'Building a cyber security culture for resilient organizations against cyber

attacks', *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi*, 7(1), pp. 96–110.

Aldawood, H. and Skinner, G. (2019) 'Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues', *Future internet*, 11(3), p. 73.

Alex-Omiogbemi, A.A. *et al.* (2024a) 'Advances in cybersecurity strategies for financial institutions: A focus on combating E-Channel fraud in the Digital era', *Journal of Cybersecurity and Financial Innovation*, 12(3), pp. 35–48.

Alex-Omiogbemi, A.A. *et al.* (2024b) 'Conceptual framework for women in compliance: Bridging gender gaps and driving innovation in financial risk management'.

Almehdhar, M. *et al.* (2024) 'Deep learning in the fast lane: A survey on advanced intrusion detection systems for intelligent vehicle networks', *IEEE Open Journal of Vehicular Technology*, 5, pp. 869–906.

Bank, W. (2022) *Tanzania Overview: Development news, research, data*. Available at: https://www.worldbank.org/en/country/tanzania/overview#:~:text=The World Bank estimates a,capita GDP contraction in 2020. (Accessed: 10 April 2022).

Basir, A.W. *et al.* (2024) 'The role of employee awareness in mitigating phishing risks in the workplace'.

Cele, N.N. and Kwenda, S. (2025) 'Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review', *Journal of Financial Crime*, 32(1), pp. 31–48.

Chhabra Roy, N. (2024) 'Proactive cyber fraud response: a comprehensive framework from detection to mitigation in banks', *Digital Policy, Regulation and Governance*, 26(6), pp. 678–707.

Chika, O.V., Promise, E. and Werikum, E. V (2022) Influence of liquidity and profitability on profits growth of Nigerian pharmaceutical firms', *Goodwood Akuntansi dan Auditing Reviu*, 1(1), pp. 1–13.

Cohen, J. (1988) 'Statistical power analysis for the behavioral sciences. Lawrence Erlbaum Associates', *Hillsdale, NJ*, pp. 20–26.

Deloitte (2023) *Global Future of Cyber Survey: Building long-term value by putting cyber at the heart of the business*. Available at: https://www.deloitte.com/content/dam/assets-shared/docs/services/risk-advisory/2023/gx-deloitte_future_of_cyber_2023.pdf.

Diamantopoulos, A., Riefler, P. and Roth, K.P. (2008) 'Advancing formative measurement

models', *Journal of business research*, 61(12), pp. 1203–1218.

Dwight, J. (2024) 'Building Cyber Attack Trees with the Help of My LLM? A Mixed Method Study', in *Proceedings of the 2024 12th International Conference on Computer and Communications Management*, pp. 132–138.

Ebenezer, A.J., Paula, A.M. and Allo, T. (2016) 'Risk and investment decision making in the technological age: A dialysis of cyber fraud complication in Nigeria', *International Journal of Cyber Criminology*, 10(1), p. 62.

Gueorgiev, V. *et al.* (2025) 'Evaluating Cybersecurity Risks of Bulgaria's Energy Sector: Focus on PV and HVAC-R', *Applied Sciences*, 15(12), p. 6672.

Haag, S., Siponen, M. and Liu, F. (2021) 'Protection motivation theory in information systems security research: A review of the past and a road map for the future', *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, 52(2), pp. 25–67.

Hair, J.F., Sarstedt, M. and Ringle, C.M. (2019) 'Rethinking some of the rethinking of partial least squares', *European Journal of Marketing*, 53(4), pp. 566–584. Available at: https://doi.org/10.1108/EJM-10-2018-0665.

Hair Jr, J.F. *et al.* (2017) 'PLS-SEM or CB-SEM: updated guidelines on which method to use', *International Journal of Multivariate Data Analysis*, 1(2), pp. 107–123.

Hair Jr, J.F. *et al.* (2021) 'Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R: A Workbook'. Springer Nature.

Interpol (2024) *Interpol African Cyberthreat Assessment Report 2024 Outlook. By The African Cybercrime Operations Desk*. Available at: https://www.interpol.int/content/download/21048/file/24COM005030-AJFOC_Africa Cyberthreat Assessment Report_2024_complet_EN v4.pdf.

Ismail, W.S. (2024) 'Threat detection and response using AI and NLP in cybersecurity', *J. Internet Serv. Inf. Secur.*, 14(1), pp. 195–205.

Jegede, O.O. *et al.* (2016) 'On the link between human capital, innovation and performance: evidence from a resource-based economy', *International Journal of Learning and Intellectual Capital*, 13(1), pp. 27–49.

Karanja, E. and Rosso, M.A. (2017) 'The chief information security officer: An exploratory study', *Journal of International Technology and Information Management*, 26(2), pp. 23–47.

Kayumbe, E. and Gilliard, E. (2024) 'Cybersecurity in Tanzania: Opportunities and challenges',

International Journal for Multidisciplinary Research, 6(1), pp. 23–29.

Khan, I.A. *et al.* (2022) 'Enhancing IIoT networks protection: A robust security model for attack detection in Internet Industrial Control Systems', *Ad Hoc Networks*, 134, p. 102930.

Kline, R.B. (2016) 'Principles and Practice of Structural Equation Modeling (Fourth; TD Little, Ed.)'. New York (UK): The Guilford Press.

Kock, N. (2015) 'Common method bias in PLS-SEM: A full collinearity assessment approach', *International Journal of e-Collaboration (ijec)*, 11(4), pp. 1–10.

Li, Y. *et al.* (2022) 'Healthcare data quality assessment for cybersecurity intelligence', *IEEE Transactions on Industrial Informatics*, 19(1), pp. 841–848.

Lie, L.B., Utomo, P. and Winarno, P.M. (2021) 'Investigating the impact of cybersecurity culture on employees' cybersecurity protection behaviours: a conceptual paper', in *Conference Series*, pp. 295–305.

Mcanyana, W., Brindley, C. and Seedat, Y. (2020) 'Insight into the cyberthreat landscape in South Africa', *Accenture. Retrieved June*, 10, p. 2022.

Mehta, A. (2021) 'Impact of technological advancements on banking frauds: A case study of Indian banks', *emergence*, p. 11.

Mhina, J.R.A. and Lashayo, D.M. (2024) 'Examining the influence of online service usage habits on long-term intention to use virtual fiscal device systems in Tanzania: a taxpayer's perspective', *International Journal of Electronic Governance*, 16(1), pp. 52–73.

Nyamwihula, B. (2024). *Examining the awareness of mobile money users and their perception of cyber fraud risks: Evidence from Airtel Tanzania*. East Journal of Technological and Applied Sciences, 6(1), 90–105. https://ejtas.com/index.php/journal/article/view/1312

Mwemezi, J. and Mandari, H. (2024) 'Big data analytics usage in the banking industry in Tanzania: does perceived risk play a moderating role on the technological factors', *Journal of Electronic Business & Digital Economics* [Preprint].

Mwita, P.S. and Mhina, J.R.A. (2023) 'Assessing the Effectiveness of the Implementation of Cybercrimes Mitigation Strategies in Selected Commercial Banks in Tanzania', *European Journal of Theoretical and Applied Sciences*, 1, pp. 571–583.

Pallangyo, H.J. (2022) 'Cyber security challenges, its emerging trends on latest information and communication technology and cyber crime in mobile money transaction services', *Tanzania Journal of Engineering and Technology*, 41(2), pp. 189–204.

Podsakoff, P.M., MacKenzie, S.B. and Podsakoff, N.P. (2012) 'Sources of method bias in social science research and recommendations on how to control it', *Annual review of psychology*, 63, pp. 539–569.

Prentice-Dunn, S. and Rogers, R.W. (1986) 'Protection motivation theory and preventive health: Beyond the health belief model', *Health education research*, 1(3), pp. 153–161.

Reuters (2023) *Fraudulent transactions in 2023*. Available at: https://www.reuters.com/technology/cybersecurity/visa-prevented-40-bln-worth-fraudulent-transactions-2023-official-2024-07-23/. (Accessed: 28 May 2025).

Rojan, Z. (2024) 'Financial fraud detection based on machine and deep learning: A review', *The Indonesian Journal of Computer Science*, 13(3).

Roy, N.R. *et al.* (2024) *Cyber Security and Digital Forensics*. Springer.

Semlambo, A. and Shalua, N.S. (2024) 'Assessing Cybersecurity Threats To Tanzania's Government E-Payment Systems And Their Impact On National Security', *The Journal of Informatics*, 4(1).

Serianu (2023) *Africa Cybersecurity Report: Reimagining the African Cybersecurity Landscape*. Kenya. Available at: https://www.serianu.com/downloads/KenyaCyberSecurityReport2023.pdf.

Shmueli, G. *et al.* (2019) 'Predictive model assessment in PLS-SEM: guidelines for using PLSpredict', *European Journal of Marketing* [Preprint].

De *Silva*, B. (2023) 'Exploring the relationship between cybersecurity culture and cyber-crime prevention: A systematic review', *International Journal of Information Security and Cybercrime (IJISC)*, 12(1), pp. 23–29.

Siponen, M. *et al.* (2024) 'Protection motivation theory in information security behavior research: reconsidering the fundamentals', *Communications of the Association for Information Systems*, 53(1), pp. 1136–1165.

Soni, G. *et al.* (2022) 'A decision-making framework for Industry 4.0 technology implementation: The case of FinTech and sustainable supply chain finance for SMEs', *Technological Forecasting and Social Change*, 180, p. 121686.

Tariq, E. *et al.* (2024) 'How cybersecurity influences fraud prevention: An empirical study on Jordanian commercial banks', *International Journal of Data and Network Science*, 8(1), pp. 69–76.

Thati, B. *et al.* (2025) 'An Empirical Investigation on the Origins and Effects of Cybersecurity Culture in It Organizations.', *Journal of Cybersecurity & Information Management*, 16(1).

Tolossa, D. (2023) 'Importance of cybersecurity awareness training for employees in business', *Vidya-A Journal of Gujarat University*, 2(2), pp. 104–107.

Da Veiga, A. *et al.* (2020) 'Defining organisational information security culture—Perspectives from academia and industry', *Computers & Security*, 92, p. 101713.

Victory, C.O., Promise, E. and Mike, C.N. (2022) Impact of cyber-security on fraud prevention in Nigerian commercial banks', *Jurnal Akuntansi, Keuangan, dan Manajemen*, 4(1), pp. 15–27.

Wang, Y. *et al.* (2024) 'CEO tenure and environmental fraud for listed family firms', *Business Strategy and the Environment*, 33(3), pp. 1887–1905.

Yadav, S., Saini, R. and Sahu, P. (2024) 'Cybersecurity Threats', *Innovative Computing and Communications: Proceedings of ICICC 2024, Volume 6*, 1043, p. 1.