Journal of Mathematics and Informatics
Vol. 29, 2025, 1-16
ISSN: 2349-0632 (P), 2349-0640 (online)
Published 22 October 2025
www.researchmathsci.org
DOI:http://dx.doi.org/10.22457/jmi.v29a01258

Journal of
Mathematics and Informatics

The Influence of Cybersecurity Preventive Controls on the Effectiveness of Data Protection in Commercial Banks: A Case of NMB Bank PLC

***Fikiri Lucas Matonya*[1*] and *Paul Dotto Mazoya*[2]**

[1,2]Institute of Accountancy Arusha (IAA), Dar Es Salaam- Tanzania.
[1]Email: **fikiri.matonya@iaa.ac.tz**; [2]Email: **paul.mazoya@iaa.ac.tz**
*Corresponding author

Received 2 September 2025; accepted 20 October 2025

Abstract. This study explores the influence of cybersecurity preventive controls on the effectiveness of data protection in commercial banks, using NMB Bank PLC as a case study. The study is grounded in Protection Motivation Theory (PMT). A descriptive research design was employed and adopted a quantitative approach, allowing for objective measurement and statistical analysis of data collected. The targeted population consisted of 183 employees from five key departments across NMB Bank's Dar es Salaam branches. Using Yamane's formula, a sample size of 126 respondents was determined, and participants were selected through simple random sampling to ensure fairness and reduce selection bias. Data collection was conducted through structured questionnaires utilizing a five-point Likert scale. The survey method enabled efficient and consistent data collection from a broad sample. Data were analyzed using both descriptive and inferential statistics through SPSS Version 26. Descriptive statistics summarized demographic characteristics and response patterns, while multiple linear regression was applied to examine the relationships between independent variables (cybersecurity controls) and the dependent variable (data protection). The findings revealed that access control and network security had strong, statistically significant positive effects on data protection effectiveness, while staff training did not show a significant direct impact. The study concludes that while NMB Bank has made considerable efforts in cybersecurity, ongoing improvements in technology, enforcement, and management support are essential. The study contributes practical insights for banking institutions and policymakers aiming to enhance cybersecurity resilience in the face of evolving digital threats.

Keywords: Cybersecurity Controls; Data Protection; Protection Motivation Theory (PMT); Commercial Banks; NMB Bank PLC

AMS Mathematics Subject Classification (2010): 62J05, 68M25, 91B30

1. Introduction

Cybersecurity preventive controls are proactive measures and technologies implemented by organizations to protect their information systems and data from unauthorized access,

cyberattacks, and other security threats [5]. These controls include a variety of tools and practices such as firewalls, encryption, multi-factor authentication, antivirus software, intrusion detection systems, and regular security training for employees. Their primary goal is to prevent security breaches by identifying and blocking potential vulnerabilities before they can be exploited, thereby safeguarding the confidentiality, integrity, and availability of critical data and systems [26].

Globally, commercial banks face increasing vulnerability to cyber threats that jeopardize the confidentiality, integrity, and availability of sensitive customer and operational data. The 2023 IBM Cost of a Data Breach Report reveals that the global average cost of a data breach in the financial services sector reached $5.97 million, the highest among all industries. This highlights the critical importance of robust cybersecurity measures within banking institutions [13] (IBM, 2023). To counter these risks, banks globally have adopted a range of cybersecurity preventive controls such as multi-factor authentication, encryption, intrusion detection systems (IDS), and security information and event management (SIEM) tools [15]. For example, the European Union's General Data Protection Regulation (GDPR) has compelled banks across Europe to implement stringent cybersecurity protocols to protect data privacy and security (European Commission, 2018). In Africa, the rapid adoption of digital banking services has outpaced the development of adequate cybersecurity frameworks, leading to increased vulnerability to cyber threats. The African Union's Digital Transformation Strategy for Africa 2020-2030 recognizes cybersecurity as a foundational pillar for digital financial inclusion but also highlights significant gaps in policy implementation across the continent [2]. African Cybersecurity Report (ACR) documented a staggering 45% increase in cyberattack incidents targeting African banks between 2019 and 2021. The most common threats included phishing, malware infections, and data breaches [29]. Countries such as South Africa, Nigeria, and Kenya have made notable strides in developing cybersecurity policies tailored to the financial sector. South Africa's Cybersecurity Hub and Kenya's National Kenya Computer Incident Response Team Coordination Centre (KE-CIRT/CC) [17] have been instrumental in enhancing the cyber resilience of banks within their jurisdictions [10].

Tanzania's banking sector has witnessed a digital transformation driven largely by the widespread use of mobile and internet banking services. According to the Bank of Tanzania Annual Report (2023), the sector experienced over 70% growth in digital transactions over the past five years. However, this increase in digital activity has been accompanied by a rise in cyber threats, including unauthorized access, data breaches, and fraud attempts (BOT, 2023). In response, the Tanzanian government has introduced measures to strengthen cybersecurity, including the establishment of the National Cybersecurity Framework (2020) and the Tanzania Computer Incident Response Team (TZ-CIRT). Despite these efforts, studies such as those by Mwogosi [21] indicate that many commercial banks in Tanzania still struggle to implement comprehensive preventive controls, mainly due to resource limitations, insufficient skilled personnel, and weak regulatory enforcement.

NMB Bank [22], one of Tanzania's largest commercial banks, has aggressively expanded its digital banking platforms and currently serves millions of customers nationwide. The NMB Annual Report (2022) indicates that over 60% of the bank's transactions were digital, which has increased its exposure to cyber risks. In response, NMB has implemented various cybersecurity preventive controls including biometric

authentication, encrypted mobile banking applications, real-time transaction monitoring, and regular cybersecurity training for staff [8]. However, 2023 internal audit highlighted incidents of attempted phishing attacks and malware infections, revealing vulnerabilities in the bank's preventive controls, especially in real-time threat detection and incident response capabilities (NMB Internal Audit Report, 2023).

This study was specifically assessing how cybersecurity preventive controls influence the effectiveness of data protection within NMB Bank [22], considering both technological measures and organizational practices. By providing empirical insights from one of Tanzania's leading commercial banks, the research aims to enhance understanding of the current status of cybersecurity controls in Tanzanian banking, identify challenges and gaps in data protection, and offer recommendations to strengthen cybersecurity frameworks. The study's contribution is expected to inform policymakers, banking sector stakeholders, and cybersecurity professionals in Tanzania, helping to build more resilient commercial banks capable of mitigating the growing cyber threats in an increasingly digital financial environment.

2. Literature review

2.1. Theoretical literature review

Protection Motivation Theory (PMT) explains how individuals are motivated to adopt protective behaviors in response to perceived threats. The theory posits that protection motivation arises from two cognitive processes: threat appraisal (perceived severity and vulnerability of the threat) and coping appraisal (perceived effectiveness of the protective behavior, self-efficacy, and response cost) as explained by Marikyan et al. [19]. In the context of this study, PMT is relevant because it helps explain how employees and management at NMB Bank respond to cybersecurity threats. If they perceive cyberattacks as severe and believe they are vulnerable, and if they have confidence in the effectiveness of cybersecurity preventive controls such as encryption, real-time monitoring, and multi-factor authentication, they are more likely to comply with security protocols [9]. Thus, PMT supports the idea that the effectiveness of data protection depends not only on the availability of cybersecurity measures but also on the motivation and willingness of individuals within the bank to use them properly.

2.2. Empirical review

Al-Fadl et al., [3] conducted study focusing on the Impact of Cybersecurity Spending on the Performance in Egyptian Commercial Banks with a Field Study. Utilizing a mixed-methods approach that combined deductive and inductive reasoning. A random sample of 220 participants was drawn, resulting in 180 valid responses (82% response rate). The Kruskal-Wallis Test was employed to evaluate differences in perceptions among respondents. The findings revealed that cybersecurity investments significantly reduce cyber risks, with the highest impact seen in spending on cybercrime prevention and detection (average rating of 4.57), followed by cybersecurity development (4.54). The study further demonstrated that reducing cyber risks leads to improved bank performance, especially financial performance, which received the highest average score of 4.88. No significant differences were found in perceptions among respondents. In conclusion, the

study underscores the vital role of sustained cybersecurity investment in safeguarding banks against cyber threats and improving overall performance.

Faforiji et al., [11] conducted study focusing on the Cybersecurity Threats and Financial Performance of Listed Commercial Banks in Nigeria. The study adopted an ex-post facto research design, using a judgmental sampling technique to select ten out of the fourteen listed commercial banks on the Nigerian Exchange Limited. Secondary data were gathered from audited annual financial statements, Nigeria Deposit Insurance Corporation (NDIC) annual reports, and Nigeria Inter-Bank Settlement System (NIBSS) fraud reports covering the period from 2012 to 2023. Data analysis involved both descriptive statistics and inferential analysis using robust least square regression. The findings revealed that financial losses due to cybersecurity threats have a significant negative impact on the earnings per share of the listed banks ($\beta = -0.013024$, $p = 0.0000$), confirming that cyber threats translate into direct financial setbacks for financial institutions. The study concluded that cybersecurity risks are not merely technical issues but pose critical financial implications that can adversely affect profitability.

John et al. [16] conducted study focusing on the Assessing the Impact of IT Governance Frameworks on Cybersecurity in Nigerian Commercial Banks. The study adopted a qualitative research methodology, utilizing document analysis and expert interviews with IT and risk management professionals from selected Nigerian commercial banks. The findings revealed that banks with mature IT governance structures were better equipped to anticipate, prevent, and respond to cyber threats compared to those with fragmented or poorly integrated frameworks. However, the study also highlighted several challenges, including limited expertise, insufficient budget allocations, and inconsistent regulatory compliance. In conclusion, the study emphasized that while IT governance frameworks are essential for effective cybersecurity, their success depends on continuous refinement and integration into overall corporate governance.

Aderinto et al., [1] conducted study focusing on the Cybersecurity Threats and Financial Performance of Listed Commercial Banks in Nigeria. Adopting an ex-post facto research design, the study sampled ten out of fourteen listed commercial banks on the Nigerian Exchange Limited through judgmental sampling, utilizing secondary data from audited financial statements, Nigeria Deposit Insurance Corporation annual reports, and Nigeria Inter-Bank Settlement System fraud reports covering the period 2012 to 2023. Findings from descriptive statistics and robust least square regression revealed that financial losses from cybersecurity threats significantly and negatively impact banks' earnings per share ($\beta = -0.013024$, $p = 0.0000$), highlighting the direct financial implications of cyber risks. The study concluded that cybersecurity threats are not merely technical issues but major financial concerns that erode profitability and shareholder value. Tariq et al., (2024) conducted study focusing on the How cybersecurity influences fraud prevention: An empirical study on Jordanian commercial banks. Using a quantitative research approach, data were collected from 173 information technology managers of commercial banks listed on the Amman Stock Exchange, and Structural Equation Modeling (SEM) was applied to test the hypotheses. The findings revealed that cybersecurity significantly enhances fraud prevention, with the detect function having the strongest impact among the five dimensions. The study concluded that robust cybersecurity frameworks are critical in combating the growing sophistication of fraud in the banking sector. It recommended that Jordanian commercial banks adopt advanced measures such

as multi-factor authentication (MFA) for customer accounts, employee access, and biometric verification systems to strengthen protection against unauthorized access and safeguard sensitive information.

Senanu [26] conducted study focusing on the Cybersecurity response capabilities: a case study of commercial banks in Ghana. Employing a mixed-methods research design, data were collected from IT and Cybersecurity Managers of ten purposively selected commercial banks through questionnaires containing both open- and closed-ended items. The findings showed that the most common cyberattacks faced by banks included phishing, social engineering, botnets, ransomware, and cyber fraud, which negatively affected customer confidence in the affected banks. The study concluded that while banks have implemented several cybersecurity response measures, challenges remain in effectively addressing the evolving nature of cyber threats. It recommended enhancing cybersecurity awareness, strengthening information access and protection protocols, and investing in continuous capacity development to improve the resilience of banks against cyberattacks.

2.3. Conceptual framework

A conceptual framework is a theoretical model that outlines the key variables being examined and the connections between them. It shows how the dependent variable is influenced by the independent variable, emphasizing that changes in the independent variable affect the outcome of the dependent variable, as represented in the figure below.

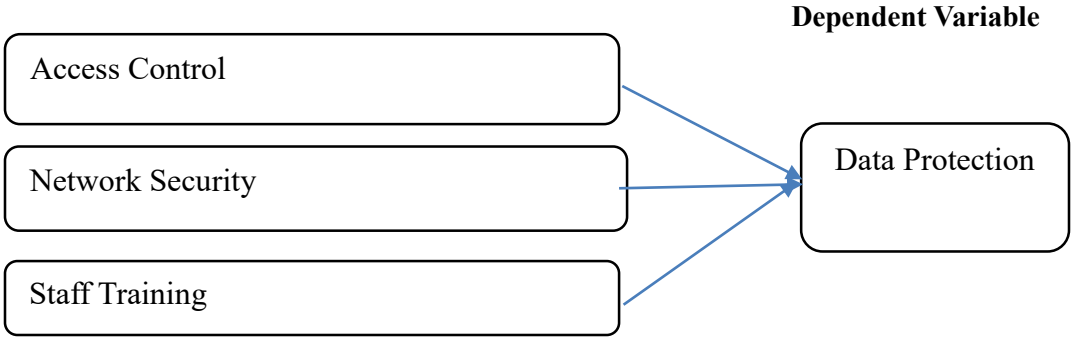

Figure 1: Conceptual framework independent variable
Source; *From Literature Review*

3.0. Methodology

3.1. Area of the study

This study was conducted in NMB Bank PLC, one of the largest and most technologically advanced commercial banks in Tanzania. The first reason for selecting NMB Bank PLC as the study area is its rapid digital transformation, with over 60% of its transactions conducted through digital platforms, making it highly exposed to cyber threats. Secondly, NMB's national reach and large customer base provide a rich context for assessing the effectiveness of cybersecurity preventive controls across diverse banking operations. Thirdly, recent internal audits and reported cyber incidents within the bank highlight

practical challenges and gaps in data protection, making NMB an ideal case for evaluating the relationship between cybersecurity controls and data security effectiveness.

3.2. Research design

The study adopted a descriptive research design, which involves systematically observing and documenting the characteristics or behaviors of a given population without altering any variables. This approach was intended to present a precise and comprehensive representation of the subject matter by collecting both quantitative and qualitative data through methods such as surveys, interviews, and observations. The descriptive design was selected as it enabled a thorough and structured examination of the research topic [18].

3.3. Research approach

This research employed a quantitative approach to examine the influence of cybersecurity preventive controls on the effectiveness of data protection in commercial banks, specifically focusing on NMB Bank PLC. The quantitative methodology involved the use of numerical data to analyze the relationships between key variables. It emphasized structured data collection tools, statistical analysis, and measurable indicators to test hypotheses and address the research questions. This approach was selected due to its reliability, validity, and effectiveness in identifying cause-and-effect relationships, making it well-suited for the study's objectives and context [7].

3.4. Targeted population

In this study, the population refers to the entire group of individuals or entities that share specific characteristics relevant to the research. This group comprises all the elements to which the study's findings are intended to be generalized. Based on data from NMB Bank in Dar es Salaam Branches (2025) the population size is identified as 183, as presented in Table 3.1.

Table 3.1: Distribution population

Department	**Number of Employees**	**Percentage (%)**
IT and Security	51	27.3%
Risk and Compliance	39	21.9%
Operations	43	24.6%
Finance and Accounts	32	16.4%
Customer Service	18	9.8%
Total	**183**	**100%**

Source; NMB Bank (2025).

3.5. Sample size and sampling techniques

3.5.1 Sample size

In this study, the sample size was determined to balance the feasibility of data collection with the need for statistical power to ensure that the findings are both reliable and generalizable.

n=N/(1+N(e^2))

n=183/ (1+183(〖0.05〗 ^2))

n=126.

3.5.2 Sampling strategies

The study utilized Simple Random Sampling as the sampling technique. This approach guarantees that every member of the population has an equal probability of selection, emphasizing its fairness and ease of application. Simple random sampling was chosen because it reduces selection bias by ensuring equal inclusion chances for all individuals. Its straightforward nature helps to obtain a sample that truly reflects the population, thereby supporting the reliability and validity of the study findings on the influence of cybersecurity preventive controls on data protection effectiveness at NMB Bank PLC [27].

3.6. Data collection methods

This study employed a survey as the primary method for data collection, with a questionnaire serving as the key instrument. Surveys are well-suited for collecting organized and systematic information from a broad and varied sample, facilitating the examination of trends, patterns, and relationships among variables. The questionnaire was structured using a Likert scale, enabling efficient and reliable measurement of participants' attitudes, perceptions, and behaviors related to cybersecurity preventive controls and data protection. This standardized format promotes consistency in responses, supports robust statistical analysis, and aids in drawing valid and meaningful conclusions about the effectiveness of data protection in commercial banks, specifically at NMB Bank PLC [20].

3.7. Data analysis methods

The study employed both descriptive and inferential statistical methods to analyze the collected data. Descriptive statistics, such as measures of central tendency (mean, median, mode) and variability (range, standard deviation), were used to summarize and present the main characteristics of the data clearly. Inferential statistics, specifically multiple linear regression analysis, were applied to make generalizations about the wider population from the sample data. The analysis was performed using SPSS Version 26, providing both a detailed summary and predictive understanding of the relationships between cybersecurity preventive controls and the effectiveness of data protection in commercial banks, focusing on NMB Bank PLC [12].

3.8. Ethical considerations

Throughout the study, the researcher maintained high ethical standards by treating all participants with respect and dignity, considering cultural differences, and promoting an inclusive atmosphere. Transparency was ensured by clearly explaining the research methods and objectives, as well as disclosing any potential conflicts of interest. Participation was entirely voluntary, allowing individuals to withdraw at any point without any negative repercussions. Confidentiality was protected through secure data storage and by anonymizing personal information. Informed consent was obtained by thoroughly informing participants about the study and addressing their questions [14].

4.0 Findings

4.1. Presentation of findings

4.1.1. Response rate

The response rate involves the proportion of respondents who completed and returned research or participated in a study out of the total number of people who were invited or sampled. It is a key indicator of the survey's reliability and validity, as a higher response rate typically suggests that the results are more representative of the target population. In research, ensuring an adequate response rate is crucial for drawing meaningful and accurate conclusions as presented in Table 4.1.

Table 1.1: Response rate

Category	***Frequency***	***Percent***
Questionnaire Distributed and returned	115	91.27%
Non – response	11	8.73%
Total	***126***	***100.00***

Source: Field data (2025)

Table 4.1 shows the response rate of the study's questionnaire distribution. Out of 126 questionnaires distributed, 115 were completed and returned, representing a high response rate of 91.27%, which indicates strong participation from the respondents. Only 11 questionnaires were not returned, accounting for 8.73% non-response. This high response rate suggests that the data collected is reliable and provides a solid basis for analyzing the influence of cybersecurity preventive controls on data protection effectiveness at NMB Bank PLC.

4.2.2 Socio - demographic characteristics

Table 4.2: Socio - demographic characteristics of the respondents

Categories		***Frequency***	***Percent***
Gender of respondents	Male	65	56.5
	Female	50	43.5
	Total	***115***	***100.0***
Age group	Between 18-30 years	31	27.0
	Between 31-40 years	50	43.5
	Between 41-50 years	22	19.1
	51 Years and above	12	10.4
	Total	***115***	***100.0***
Academic qualifications	Certificate level	14	12.2
	Diploma level	29	25.2
	Graduate level	56	48.7
	Post Graduate level	16	13.9
	Total	***115***	***100.0***
Work Experiences	Less than 3 years	7	6.1
	3 to 6 years	11	9.6
	7 and above	97	84.3
	Total	***115***	***100.0***

Source; Field Data (2025).

Table 4.2 illustrates the socio-demographic profile of the 115 respondents involved in the study. In terms of gender, males constituted the majority with 56.5%, while females accounted for 43.5%, reflecting a relatively balanced gender representation among participants. This gender distribution ensures that insights into cybersecurity preventive controls at NMB Bank PLC are inclusive of diverse perspectives.

Regarding age, the largest proportion of respondents (43.5%) fell within the 31-40 years age group, followed by 27.0% in the 18-30 years bracket. Respondents aged between 41-50 years represented 19.1%, while those aged 51 years and above comprised 10.4%. This distribution indicates a predominantly young to middle-aged workforce, which may influence their familiarity and interaction with modern cybersecurity measures.

The academic qualifications of respondents showed that nearly half (48.7%) held graduate-level education, while 25.2% had diplomas. Those with postgraduate qualifications represented 13.9%, and certificate holders accounted for 12.2%. This suggests a well-educated sample capable of understanding and applying complex cybersecurity preventive controls within the bank.

Finally, the work experience data reveal that a significant majority of respondents (84.3%) have been employed at NMB Bank PLC for seven years or more, indicating substantial institutional knowledge and experience. Those with three to six years of experience made up 9.6%, while only 6.1% had less than three years of experience. This extensive work experience is likely to contribute positively to the effective implementation and management of data protection practices in the bank.

4.3. Descriptive analysis

4.3.1 The influence of cybersecurity preventive controls on the effectiveness of data protection in commercial banks at NMB bank PLC.

Table 4.3: The influence of cybersecurity preventive controls

Statements for Likert scale		Frequency	Percent	Mean	SD
The access control mechanisms implemented by the bank, such as password policies and biometric systems, effectively prevent unauthorized access to sensitive customer and operational data.	Strong Disagree	2	1.7	3.63	1.062
	Disagree	16	13.9		
	Neutral	33	28.7		
	Agree	35	30.4		
	Strong Agree	29	25.2		
	Total	***115***	***100.0***		
Encryption technologies employed by the bank sufficiently protect confidential information during data transmission and storage, reducing the risk of data breaches.	Strong Disagree	2	1.7	3.36	.948
	Disagree	23	20.0		
	Neutral	31	27.0		
	Agree	50	43.5		
	Strong Agree	9	7.8		
	Total	***115***	***100.0***		

Regular and comprehensive cybersecurity training programs for employees significantly enhance their awareness and ability to adhere to security protocols within the bank.	Strong Disagree	2	1.7	3.54	.920
	Disagree	15	13.0		
	Neutral	30	26.1		
	Agree	55	47.8		
	Strong Agree	13	11.3		
	Total	***115***	***100.0***		
The bank's intrusion detection and prevention systems (IDPS) are effective in identifying and mitigating potential cyber threats in real-time before they can cause damage.	Strong Disagree	4	3.5	3.51	1.187
	Disagree	25	21.7		
	Neutral	23	20.0		
	Agree	34	29.6		
	Strong Agree	29	25.2		
	Total	***115***	***100.0***		
Multi-factor authentication (MFA) is consistently enforced across all banking platforms, ensuring that only authorized personnel can access critical systems and customer accounts.	Strong Disagree	5	4.3	3.41	1.008
	Disagree	18	15.7		
	Neutral	28	24.3		
	Agree	53	46.1		
	Strong Agree	11	9.6		
	Total	***115***	***100.0***		
The bank's management actively supports and prioritizes investments in cybersecurity preventive controls to strengthen overall data protection and minimize cyber risks.	Strong Disagree	7	6.1	3.31	1.071
	Disagree	22	19.1		
	Neutral	24	20.9		
	Agree	52	45.2		
	Strong Agree	10	8.7		
	Total	***115***	***100.0***		
Average Mean Score				***3.46***	***1.03***

Source; Field Data (2025).

Table 4.3 presents the respondents' perceptions regarding the influence of cybersecurity preventive controls on data protection effectiveness at NMB Bank PLC. The access control mechanisms implemented by NMB Bank, such as password policies and biometric systems, are generally perceived as effective in preventing unauthorized access to sensitive customer and operational data. With a mean score of 3.63, over half of the respondents (55.6%) agreed or strongly agreed with this statement, indicating confidence in these controls. However, 15.6% of respondents expressed disagreement, highlighting that while access controls are largely effective, there may still be gaps or inconsistencies that need addressing.

Respondents showed moderate agreement (mean = 3.36) that encryption technologies used by the bank sufficiently protect confidential information during transmission and storage. A total of 51.3% agreed or strongly agreed that encryption helps

reduce data breach risks, but a significant 21.7% disagreed or strongly disagreed. This split suggests that while encryption is a key protective measure, there may be concerns about its implementation, effectiveness, or coverage that warrant further improvement.

Regular and comprehensive cybersecurity training programs are seen as valuable, with a mean score of 3.54. A majority of respondents (59.1%) agreed or strongly agreed that such training enhances employee awareness and adherence to security protocols. This reflects the important role of continuous education in strengthening human factors in cybersecurity. Nonetheless, a minority (14.7%) disagreed, which may point to variability in training quality or participation.

The bank's IDPS received a mean rating of 3.51, indicating moderate confidence in their effectiveness at identifying and mitigating cyber threats in real-time. While 54.8% agreed or strongly agreed that these systems are effective, a sizeable 25.2% disagreed, signaling that real-time threat detection might face challenges such as delayed responses, false positives, or technology limitations that need to be addressed.

MFA enforcement across banking platforms received a mean score of 3.41, with 55.7% of respondents agreeing or strongly agreeing that MFA is consistently applied to restrict access to authorized personnel only. However, 20% of respondents disagreed or strongly disagreed, suggesting inconsistencies in MFA application or user compliance issues that may reduce its overall effectiveness in preventing unauthorized access.

This statement had the lowest mean score of 3.31, indicating that management support and prioritization of cybersecurity investments are perceived as less robust compared to other controls. While 53.9% agreed or strongly agreed that management actively supports cybersecurity initiatives, 25.2% disagreed, pointing to possible gaps in resource allocation, leadership commitment, or strategic focus on cybersecurity, which could undermine overall data protection efforts.

Overall, the average mean score of 3.46 suggests a generally positive perception of cybersecurity preventive controls at NMB Bank PLC, but the variation in agreement levels across statements highlights specific areas particularly encryption, IDPS effectiveness, MFA enforcement, and management support that require continued attention to strengthen the bank's data protection framework.

4.4. Regression analysis

Table 4.4: Coefficients of the variables

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	.847	.157		5.393	.000	.536	1.158
	Access Control	.507	.066	.574	7.631	.000	.375	.639
	Network Security	.240	.046	.341	5.274	.000	.150	.331
	Staff Training	.025	.052	.032	.487	.627	-.077	.128
	Dependent Variable; Data Protection							

Source; Field Data (2025).

Table 4.4 presents the regression coefficients analyzing the influence of cybersecurity preventive controls on data protection at NMB Bank PLC. The constant term is significant (B = 0.847, p < 0.001), indicating the baseline level of data protection when all independent variables are zero. Access control has a strong, positive, and statistically significant effect on data protection (B = 0.507, β = 0.574, p < 0.001), suggesting that improved access control mechanisms substantially enhance data protection effectiveness. Network security also shows a significant positive impact (B = 0.240, β = 0.341, p < 0.001), indicating that robust network security measures contribute meaningfully to safeguarding data. However, staff training does not have a statistically significant effect on data protection in this model (B = 0.025, β = 0.032, p = 0.627), implying that training alone, as measured here, may not directly influence data protection outcomes. Overall, these results highlight the critical roles of access control and network security in enhancing data protection, while the effect of staff training may depend on other factors not captured in this model.

Table 4.5: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.860[a]	.739	.732	.4332017

Source; Field Data (2025)

.

Table 4.5 presents the model summary for the regression analysis examining the influence of cybersecurity preventive controls on data protection at NMB Bank PLC. The model shows a strong positive correlation between the independent variables and data protection, with an R value of 0.860, indicating a high degree of association. The R Square value of 0.739 means that approximately 73.9% of the variation in data protection effectiveness can be explained by the combined influence of the cybersecurity preventive controls included in the model. The Adjusted R Square of 0.732, which accounts for the number of predictors, confirms that the model provides a good fit to the data. Additionally, the standard error of the estimate at 0.433 suggests that the predictions made by the model are reasonably accurate. Overall, this model demonstrates a strong explanatory power of cybersecurity preventive controls on data protection effectiveness in the bank.

Table 4.6: ANOVA

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	59.056	3	19.685	104.897	.000[b]
	Residual	20.831	111	.188		
	Total	***79.887***	***114***			

Source: Field Data (2025).

Table 4.6 presents the ANOVA results for the regression model assessing the influence of cybersecurity preventive controls on data protection at NMB Bank PLC. The regression sum of squares (59.056) reflects the variation explained by the model, while the residual sum of squares (20.831) represents unexplained variation. With 3 degrees of freedom for the regression and 111 for the residuals, the mean square for the regression is 19.685, which

is substantially higher than the residual mean square of 0.188. The F-statistic value of 104.897 is highly significant ($p < 0.001$), indicating that the overall regression model is statistically significant and that the independent variables collectively provide a strong explanation of the variability in data protection effectiveness. This confirms that cybersecurity preventive controls significantly impact data protection in the bank.

5. Discussion

The findings of this study reveal that cybersecurity preventive controls play a crucial role in enhancing the effectiveness of data protection at NMB Bank PLC. Access control mechanisms are widely recognized by respondents as a key factor in preventing unauthorized access to sensitive data, underscoring their importance in securing banking operations. Similarly, network security measures contribute significantly to safeguarding data, confirming the critical role of robust technological defenses. However, while staff training is acknowledged as beneficial for raising awareness and adherence to security protocols, its direct impact on data protection appears limited within this context, suggesting that training alone may not suffice without complementary technical controls. The effectiveness of intrusion detection and prevention systems receives mixed perceptions, indicating potential challenges in real-time threat identification and mitigation that warrant further improvement. Additionally, although multi-factor authentication is generally enforced, inconsistencies in its application highlight areas where security protocols could be strengthened to prevent unauthorized access. Management support for cybersecurity initiatives, while acknowledged, is perceived as less consistent, suggesting that stronger leadership commitment and resource allocation are needed to sustain and enhance cybersecurity efforts. Overall, these findings highlight that while NMB Bank has implemented various preventive controls, ongoing attention to technological enhancements, employee engagement, and managerial commitment is essential to fortify data protection and effectively counter evolving cyber threats.

This output is similarly with the study of John et al., (2024) which revealed that banks with mature IT governance structures were better equipped to anticipate, prevent, and respond to cyber threats compared to those with fragmented or poorly integrated frameworks. However, the study also highlighted several challenges, including limited expertise, insufficient budget allocations, and inconsistent regulatory compliance.

6. Conclusion

In conclusion, this study underscores the significant influence of cybersecurity preventive controls on the effectiveness of data protection at NMB Bank PLC. Strong access control and network security measures emerge as critical components in safeguarding sensitive banking information, while employee training, although important for awareness, requires integration with robust technical controls to maximize its impact. The mixed perceptions around intrusion detection systems and multi-factor authentication highlight the need for continuous improvements and consistent enforcement to address evolving cyber threats effectively. Furthermore, the findings point to a vital role for management in prioritizing and adequately resourcing cybersecurity initiatives to sustain a resilient defense framework. Strengthening these areas not only enhance data protection but also build

greater trust and confidence among customers and stakeholders in the bank's ability to secure their information.

7. Recommendations

Based on the findings of this study, it is recommended that NMB Bank PLC strengthen its access control mechanisms by regularly reviewing and updating password policies and biometric authentication systems to address any emerging vulnerabilities. Ensuring strict enforcement and periodic audits of access permissions can further minimize the risk of unauthorized data access. Additionally, the bank should invest in advanced network security technologies and continuously monitor their effectiveness to safeguard against sophisticated cyber threats, including malware and intrusion attempts.

Furthermore, while staff training programs are valuable, the bank should enhance these initiatives by tailoring training content to specific roles and incorporating practical simulations of cyberattack scenarios. This approach help employees better understand their responsibilities and improve their readiness to respond to security incidents. Coupling training with ongoing assessments and refresher courses can maintain high levels of cybersecurity awareness and compliance across the organization.

Lastly, it is crucial for NMB Bank's management to demonstrate stronger commitment to cybersecurity by allocating sufficient resources and prioritizing investments in preventive controls such as multi-factor authentication and intrusion detection systems. Establishing a dedicated cybersecurity governance team to oversee the implementation, monitoring, and continuous improvement of security measures ensure a proactive and coordinated approach. This strategic focus not only enhance data protection but also reinforce customer trust and safeguard the bank's reputation in an increasingly digital banking environment.

Acknowledgements. The authors would like to thank the anonymous referees and the editor for their crucial comments for improvement of the paper.

Conflicts of interest. The authors declare no conflicts of interest.

Authors' contributions. All authors contributed equally to this work.

REFERENCES

1. A. Aderinto and A. Faforiji, Cybersecurity threats and financial performance of listed commercial banks in Nigeria, *Asian Journal of Advanced Research and Reports*, 19 (2025) 381–394. https://doi.org/10.9734/ajarr/2025/v19i4990.
2. African Union, *Digital Transformation Strategy for Africa (2020–2030)*, African Union, Addis Ababa, (2020). https://au.int/en/documents/20200603/digital-transformation-strategy-africa-2020-2030.
3. A. Al-Fadl, A. Ibrahim, and M. Eid, The impact of cybersecurity spending on performance in Egyptian commercial banks: A field study, *Journal of Lifestyle and SDGs Review*, 5 (2025) e06024. https://doi.org/10.47172/2965-730X.SDGsReview.v5.n04.pe06024.

4. Bank of Tanzania, *Annual Report 2022/2023*, Bank of Tanzania, Dar es Salaam, (2023). https://www.bot.go.tz/Publications/Filter/23.
5. H. Blake, AI-powered threats in supply chains: A looming cybersecurity challenge, *Journal of Cybersecurity Studies*, (2025).
6. K. Dehalwar and S. Sharma, Fundamentals of research writing and uses of research methodologies, *Open Science Repository*, (2023). https://doi.org/10.5281/zenodo.10117851.
7. U. K. B. Dubey and D. P. Kothari, *Research Methodology: Techniques and Trends*, Chapman and Hall/CRC, Boca Raton, (2022).
8. E. Edim and A. Udofot, Assessment of cybersecurity threats of using portable devices in banking services, *International Journal of Science and Research Archive*, 14 (2025) 824–833. https://doi.org/10.30574/ijsra.2025.14.3.0472.
9. F. Estebsari, Z. R. Khalifehkandi, M. Latifi, A. Farhadinasab, P. Vasli, and D. Mostafaie, Protection motivation theory and prevention of breast cancer: A systematic review, *Clinical Breast Cancer*, 23 (2023) e239–e246.
10. European Commission, *General Data Protection Regulation (GDPR)*, Official Journal of the European Union, (2018). https://eur-lex.europa.eu/eli/reg/2016/679/oj.
11. A. Faforiji, Cybersecurity threats and financial performance of listed commercial banks in Nigeria, *Asian Journal of Advanced Research and Reports*, 19 (2025) 381–394. https://doi.org/10.9734/ajarr/2025/v19i4990.
12. T. Hamed, Different types of data analysis: Data analysis methods and techniques in research projects, *International Journal of Academic Research in Management*, 9 (2020) 1–9.
13. IBM, *Cost of a Data Breach Report 2023*, IBM Security, (2023). https://www.ibm.com/reports/data-breach.
14. R. Iphofen, Ethics and integrity in research, in: *Handbook of Research Ethics and Scientific Integrity*, Springer, (2020) 739–749.
15. N. Jansen, Enhancing cybersecurity threat prevention through information security event management (SIEM) and policy deployment effectiveness, *ResearchGate Preprint*, (2023). https://doi.org/10.13140/RG.2.2.33723.02088.
16. J. John and T. Fred, Assessing the impact of IT governance frameworks on cybersecurity in Nigerian commercial banks, *African Journal of Information Systems*, (2024).
17. KE-CIRT/CC, *Annual Cybersecurity Report 2021*, Communications Authority of Kenya, Nairobi, (2021). https://www.ke-cirt.go.ke/reports/.
18. D. Mahat, D. Neupane, and S. Shrestha, Quantitative research design and sample trends: A systematic examination of emerging paradigms and best practices, *Cognizance Journal of Multidisciplinary Studies*, 4 (2024) 20–27.
19. D. Marikyan and S. Papagiannidis, Protection motivation theory: A review, in: *Theory Hub Handbook*, (2023) 78–93.

20. J. Muguro, P. Njeri, and M. Sasaki, Data collection methods, *Open Access Book Chapter*, (2024). https://doi.org/10.2174/9789815238518124010004.
21. A. Mwogosi, Digital policy and governance frameworks for EHR systems in Tanzania: A scoping review, *Digital Policy, Regulation and Governance*, (2025). https://doi.org/10.1108/DPRG-11-2024-0289.
22. NMB Bank, *Annual Report 2022*, NMB Bank PLC, Dar es Salaam, (2022). https://www.nmbbank.co.tz/about-us/investor-relations/annual-reports.
23. NMB Bank, *Internal Audit Report 2023* (Unpublished internal document), Dares Salaam, (2023).
24. A. Rajuroy and M. Emmanuel, Digital banking and customer adoption: The impact of internet and mobile banking on financial services in Bangladesh, *Asian Journal of Digital Finance*, (2025).
25. C. Saidi, C. Kimuyu, and C. Handa, The implications of cybercrime on economic security: The case of Kenya, *International Journal of Research and Innovation in Social Science*, 8 (2024) 2464–2471. https://doi.org/10.47772/IJRISS.2024.8090204.
26. J. Senanu, Cybersecurity response capabilities: A case study of commercial banks in Ghana, *ResearchGate Preprint*, (2022). https://doi.org/10.13140/RG.2.2.33611.26400
27. L. P. Sinnappan, M. A. A. Mamun, A. A. Zemate, and M. B. Sedra, Unlocking cybersecurity value through advanced technology and analytics: From data to insight, *Journal of Information Systems Research*, 20 (2024) 202–218
28. J. A. Smith, Simple random sampling techniques, *Journal of Sampling Theory*, 16 (2020) 232–245.
29. E. Tariq, I. Akour, N. Al-shanableh, E. Alquqa, N. Alzboun, S. Ibra-Heem, S. Al-Hawary, and M. Alshurideh, How cybersecurity influences fraud prevention: An empirical study on Jordanian commercial banks, *International Journal of Data and Network Science*, 8 (2024) 69–76. https://doi.org/10.5267/j.ijdns.2023.10.016.
30. K. Yesugade, Cybersecurity challenges in the modern banking sector, *Journal of Digital Security*, 14 (2024) 92–99.