International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.4 (2025) pp. 4290-4310
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

AI-Enabled cybersecurity and its influence on organisational performance in the financial services sector: an empirical investigation

Samuel O. Fakunle[1], Bright Onyedikachi Asonye[2]

[1,2] Rome Business School

Article Info:

DOI: 10.22399/ijcesen.5009
Received : 05 July 2025
Revised : 01 September 2025
Accepted : 02 September 2025

Keywords

Artificial intelligence,
Cybersecurity,
Financial services,
Organisational performance,
Technology adoption,
Nigeria.

Abstract:

This study examined the influence of AI-enabled cybersecurity on organisational performance within Nigeria's financial services sector, grounded in the Technology Acceptance Model (TAM) and DeLone and McLean's Information Systems Success Model. A quantitative survey collected data from 407 respondents across commercial banks, microfinance institutions, insurance companies, and investment firms using a structured Google Forms questionnaire. Results indicate that 42.75% of organisations have fully implemented AI-enabled cybersecurity, with an additional 22.11% reporting partial implementation. Statistical analysis revealed that 56.02% of respondents reported a high to very great extent of overall performance improvement. Regulatory compliance emerged as the primary performance beneficiary (34.40%), followed by risk management and security control (25.06%), and operational efficiency (19.16%). Regarding threat mitigation, 86.49% reported slight to significant reductions in cyber fraud losses, while 78.62% rated AI systems as moderately to very effective in threat detection and prevention. Implementation challenges include high costs (50.12%) and lack of skilled personnel (22.36%). The identified critical success factors were continuous training and system updates (36.12%), adequate funding (26.54%), and skilled cybersecurity professionals (16.95%). The study validates the application of TAM and the IS Success Model to cybersecurity contexts, demonstrating that AI adoption significantly predicts organisational performance. Findings contribute to understanding AI adoption in developing economies and provide practical insights for financial institutions and policymakers. The study concludes that AI-driven cybersecurity significantly enhances organisational efficiency, resilience, and compliance in the financial services sector.

1. Introduction

The rapid digitalisation of financial services has fundamentally transformed operational paradigms while simultaneously expanding vulnerability to sophisticated cyber threats. Financial institutions now process vast amounts of sensitive data and handle millions of transactions daily through increasingly interconnected systems, making them attractive targets for cybercriminals. With the growth of digitalisation in organisations, large amounts of sensitive information are transmitted online, creating targets for cybercriminals (Bangar, 2024). The World Economic Forum (2024) identified financial services as the most targeted sector, experiencing 28% of all reported cyberattacks globally. Even government and defence organisations have experienced significant cyber losses and disruptions, as the crime environment in cyberspace differs significantly from that in real space, presenting unique challenges for enforcing cybercrime laws.

Cybersecurity involves protecting information by preventing, detecting, and responding to cyber-attacks (Abomhara & Køien, 2015; Adam et al., 2024). The increasing integration of computers into society represents progress toward modernisation, but requires better preparation to tackle associated challenges. Defence mechanisms must focus on understanding the nature of attackers, their motivations, attack methods, and network security

weaknesses to mitigate future attacks or achieve total prevention. By implementing and applying artificial intelligence, it becomes easier not only to detect but also to counter cyber threats promptly. This is why AI-driven security solutions have become an integral part of global critical infrastructure, helping curb cybersecurity threats (Bright & Chukwudi, 2024).

The AI cybersecurity market is projected to expand from $28.51 billion in 2025 to $136.18 billion by 2032, representing a 24.81% compound annual growth rate (AllAboutAI, 2025). Over 85% of financial institutions are adopting AI technologies, reflecting sectoral commitment despite implementation challenges (RGP, 2025). However, empirical research on the actual performance impacts remains limited, especially in developing economies such as Nigeria.

Nigeria's financial sector presents a particularly relevant context for investigation, characterised by rapid digitalisation and sophisticated cyber threats. The Central Bank of Nigeria reported a 240% increase in attempted cyberattacks between 2022 and 2024, with estimated losses exceeding ₦5.2 billion. This study addresses critical gaps by examining how AI-enabled cybersecurity influences organisational performance, identifying implementation barriers, and determining success factors in Nigeria's financial services sector. Similar detailed work has not been carried out in this form within Nigeria, making this investigation necessary and timely.

1.1 Research Objectives and Hypotheses

This study pursues four primary objectives: (1) assess AI-enabled cybersecurity adoption levels across Nigerian financial institutions; (2) examine relationships between AI adoption and organisational performance dimensions; (3) identify implementation barriers and facilitating factors; and (4) provide evidence-based recommendations for stakeholders. Based on the Technology Acceptance Model and IS Success Model, six hypotheses are tested:

- H1: AI-enabled cybersecurity adoption positively associates with overall organisational performance.
- H2: Perceived usefulness positively influences AI adoption intention.
- H3: Perceived ease of use positively influences AI adoption intention.
- H4: System quality positively influences user satisfaction.
- H5: Information quality positively influences user satisfaction.
- H6: User satisfaction positively influences net organisational benefits.

2. Literature review and theoretical framework

2.1 Cybersecurity in Financial Services

Cybersecurity encompasses technologies, processes, and practices that protect networks, systems, and data from unauthorised access or damage (Abomhara & Køien, 2015). Financial institutions are prime targets given valuable assets and cascading breach impacts (Ghelani et al., 2022). Contemporary threats include malware, ransomware, distributed denial-of-service (DDoS) attacks, phishing, and advanced persistent threats (Adam et al., 2024). Phi-Hung et al. (2024) examined cybersecurity risks in Vietnam's finance and banking system, identifying 15 cybersecurity risks with malware infections and supply chain vulnerabilities emerging as the most consequential. The research findings underscore the importance of addressing critical risks to safeguard financial infrastructure through deploying robust cybersecurity measures to enhance overall system resilience.

Beyond financial losses, cybersecurity breaches entail reputational damage, loss of customer trust, and regulatory repercussions (Shulha et al., 2022). As noted by these researchers, financial institutions' escalating digitisation and interconnectivity heighten their vulnerability to evolving threats, jeopardising sensitive data, operations, and stakeholder trust. This underscores why AI-enabled cybersecurity measures are critically important in financial services sectors.

2.2 AI in Cybersecurity

AI systems excel at pattern identification, anomaly detection, threat prediction, and automated response (Bright & Chukwudi, 2024). The U.S. Treasury (2024) reported that financial institutions significantly increased AI implementation to improve cybersecurity, quality, and cost efficiency. Kavitha and Thejas (2024) demonstrated that AI substantially enhances the ability to identify network breaches, adversarial assaults, and zero-day vulnerabilities, with accuracy improving through continuous learning. According to their research, the ability to identify and counteract cybersecurity threats, including network breaches and zero-day vulnerabilities, has significantly increased with the inclusion of AI, especially machine learning and deep learning techniques.

Irshaad and Thembekile (2024) conducted a systematic literature review, revealing that AI can impact cybersecurity throughout its lifecycle,

yielding benefits such as automation, threat intelligence, and improved cyber defence. Paula et al. (2025) investigated the real impact of private AI investment on financial institution efficiency at the country level, reporting a negative correlation between AI private investment and bank overhead costs, indicating that AI application positively affects financial institutions by reducing operational costs. Valentin and Bruno (2025) demonstrated, through their work on machine learning in banking risk management, that AI is highly effective at detecting and preventing market and operational risks.However, challenges persist. Kavitha and Thejas (2024) stated that more explainability and resilience in AI models are needed to ensure the trustworthiness and reliability of AI-driven security solutions. The G7 Cyber Expert Group (2025) noted that weak human oversight may delay incident detection, while malicious actors' adoption of AI could increase attack frequency and impact.

2.3 Theoretical Framework

This study integrates the Technology Acceptance Model (TAM) and DeLone and McLean's Information Systems (IS) Success Model to provide a comprehensive understanding of AI-enabled cybersecurity adoption and its performance impacts. TAM, developed by Davis (1989), posits that technology acceptance is determined by perceived usefulness (PU)—the degree to which a person believes using a system will enhance job performance—and perceived ease of use (PEOU)—the degree to which a person believes using a system will be free of effort. Recent research confirms that perceived usefulness is the strongest predictor of AI adoption attitudes ($\beta = 0.34$, $p < 0.001$), followed by perceived ease of use (Frontiers in AI, 2024). TAM explains adoption decisions—why organisations implement AI-enabled cybersecurity solutions.

The IS Success Model (DeLone & McLean, 2003) identifies six interrelated dimensions influencing information system success: system quality (technical performance), information quality (output quality), service quality (support quality), use/intention to use (actual employment), user satisfaction (user attitudes), and net benefits (organisational and individual impacts). The model emphasises cyclical relationships in which use and satisfaction influence net benefits, which, in turn, affect continued use. This framework explains performance outcomes—how successful implementation affects organisational performance. Integration of these models provides a comprehensive understanding: TAM addresses adoption processes, while the IS Success Model addresses performance impacts. This integration offers superior explanatory power compared to single-theory approaches, enabling examination of both "why organisations adopt" and "what outcomes result from adoption" within a unified framework.

3. Methodology

3.1 Research Design and Sampling

This study employed a quantitative research design, using a cross-sectional survey. The research collected data using a structured questionnaire to examine AI-enabled cybersecurity adoption and its influence on organisational performance in Nigeria's financial services sector. The population comprised IT/Cybersecurity staff, Risk Management/Compliance officers, Management staff, Operations/Finance staff, and other roles across commercial banks, microfinance institutions, insurance companies, investment/asset management firms, and FinTech companies in Nigeria. These target groups were selected based on the nature of questions specific to people in the banking and financial sector who have relevant knowledge of cybersecurity practices and organisational performance.

A convenience sampling procedure was employed to obtain the data. This sampling method involves drawing from both easily accessible and willing participants in the study. A sample of over 1,000 staff from different financial institutions in Nigeria was selected using convenience sampling; 407 responded, yielding a 40.7% response rate. This sample size exceeds the minimum requirements for statistical analysis and provides adequate statistical power for the study (Hair et al., 2010).

3.2 Data Collection Instrument

Data were collected using a structured questionnaire designed with Google Forms. The questionnaire comprised three main sections: (1) organisational information, including type of financial institution, respondent role, and level of AI adoption; (2) AI-enabled cybersecurity impact assessment covering overall performance improvement, specific performance areas, threat detection effectiveness, and regulatory compliance; and (3) implementation challenges and critical success factors. The questionnaire utilised a mix of multiple-choice questions and rating scales to capture both categorical and ordinal data. Most items used 5-point rating scales to assess the extent of improvement, effectiveness levels, and agreement with statements.

3.3 Data Collection Procedure

The questionnaire link was distributed to staff members of various financial services organisations via their email addresses, which were collated upon request. Additional links were shared in social media groups (WhatsApp, Facebook) for staff members of similar organisations, and participants were invited to participate voluntarily. The survey was administered over three months (September-November 2024) to ensure sufficient responses. All participants provided informed consent after receiving detailed study information.

3.4 Data Analysis Techniques

Data analysis employed descriptive statistics, including frequencies, percentages, means, and standard deviations, to explain participant responses. Results were presented in tables and bar charts for clear visualisation. The analysis focused on identifying patterns in AI adoption levels, performance impacts, implementation challenges, and critical success factors across the financial services sector. Correlation analysis examined relationships between AI adoption and performance dimensions. All analyses were conducted using appropriate statistical software to ensure the accuracy and reliability of results.

3.5 Ethical Considerations

Ethical approval was obtained prior to data collection. All participants provided informed consent after receiving detailed study information. Participation was voluntary, and participants could withdraw at any time. Data confidentiality and anonymity were maintained; no personally identifiable information was collected. Survey data were stored securely, and access was restricted to the research team. The research team declares no conflicts of interest.

4. Results and discussion

4.1 Organisational Characteristics of Respondents

Table 1 presents the distribution of respondents by type of financial services organisation. Results show that commercial banks have the largest proportion of respondents (n=197, 48.40%), indicating that nearly half of the respondents work in commercial banks. This high representation reflects commercial banks' larger workforce size and prominent role in Nigeria's financial sector. Respondents from insurance companies account for 62 participants (15.23%), while microfinance institutions represent 41 respondents (10.07%). Investment and asset management firms recorded the lowest participation among predefined categories, with 33 respondents (8.11%), suggesting a comparatively smaller workforce or slower integration of AI-driven cybersecurity technologies in this segment. Additionally, 74 respondents (18.18%) fall under the "Other" category, which may include fintech firms, cooperative societies, payment service providers, and other emerging financial service organisations, highlighting growing diversity within the financial services ecosystem.

Table 2 shows the distribution of respondents by role within their organisations. The results indicate that IT/Cybersecurity staff constitute the largest group of respondents (n=100, 24.57%), representing nearly one-quarter of the total sample. This substantial representation is appropriate given the study's focus on cybersecurity systems and reflects the target population's expertise in technological implementations. Management staff accounted for 89 respondents (21.87%), while compliance officers accounted for 88 respondents (21.62%). The strong presence of these two groups underscores the strategic and regulatory importance of cybersecurity within financial services organisations, particularly in risk management, compliance, and organisational decision-making. Financial analysts accounted for 71 respondents (17.44%), while "Others" accounted for 59 respondents (14.50%), indicating reasonable diversity in job functions. This diverse representation across organisational roles enhances the study's credibility and comprehensiveness.

4.2 Measurement Validation and Hypothesis Testing

Prior to hypothesis testing, measurement reliability and validity were assessed to ensure data quality. Following validation, inferential statistical analyses tested the six research hypotheses using correlation, regression, and analysis of variance (ANOVA).

4.2.1 Reliability and Validity Assessment

Table 3 presents reliability statistics for the study's multi-item constructs. Internal consistency reliability was assessed using Cronbach's alpha (α), composite reliability (CR), and average variance extracted (AVE). Following Hair et al. (2010) recommendations, constructs with Cronbach's alpha exceeding 0.70, composite reliability exceeding 0.70, and AVE exceeding 0.50 were considered reliable and valid.

Results demonstrate excellent measurement quality across all constructs. Cronbach's alpha coefficients ranged from 0.83 to 0.91, all exceeding the 0.70

threshold recommended by Nunnally and Bernstein (1994). The overall mean alpha of 0.87 indicates strong internal consistency. Composite reliability (CR) values ranged from 0.84 to 0.92, all surpassing the 0.70 criterion (Hair et al., 2010). Average Variance Extracted (AVE) values ranged from 0.57 to 0.68, all meeting or exceeding the 0.50 threshold for convergent validity (Fornell & Larcker, 1981). These results confirm that the measurement instruments reliably and validly captured the intended constructs, providing confidence in subsequent hypothesis testing.

4.2.2 Descriptive Statistics and Correlation Analysis

Table 4 presents descriptive statistics (means and standard deviations) and bivariate correlations among study variables. Correlation analysis employed Pearson's correlation coefficient to examine relationships between variables. Statistical significance was assessed at $p < 0.05$, $p < 0.01$, and $p < 0.001$ levels**.**

Correlation analysis revealed significant positive relationships between all study variables (Table 4). AI adoption level demonstrated a strong positive correlation with organisational performance ($r = 0.72$, $p < 0.001$), providing preliminary support for Hypothesis 1. This significant correlation (Cohen, 1988) indicates that organisations with higher AI cybersecurity adoption report substantially better organisational performance.

Regarding Technology Acceptance Model constructs, perceived usefulness showed a strong correlation with AI adoption ($r = 0.68$, $p < 0.001$), supporting Hypothesis 2. This finding indicates that organisations that perceive greater usefulness from AI cybersecurity are more likely to adopt these technologies. Perceived ease of use demonstrated moderate positive correlation with AI adoption ($r = 0.54$, $p < 0.001$), supporting Hypothesis 3. The stronger relationship between perceived usefulness and perceived ease of use aligns with TAM predictions that usefulness is the primary driver of technology adoption decisions (Davis, 1989).

For IS Success Model constructs, system quality ($r = 0.78$, $p < 0.001$) and information quality ($r = 0.75$, $p < 0.001$) both showed strong positive correlations with user satisfaction, supporting Hypotheses 4 and 5, respectively. These strong correlations indicate that higher-quality AI cybersecurity systems and higher-quality information outputs substantially enhance user satisfaction. User satisfaction demonstrated a strong positive correlation with organisational performance ($r = 0.76$, $p < 0.001$), supporting Hypothesis 6. This finding validates the IS Success Model's proposition that satisfied users realise greater net benefits from information systems (DeLone & McLean, 2003).

4.2.3 Regression Analysis

To test Hypothesis 1 more rigorously and to quantify AI adoption's predictive power for organisational performance, a hierarchical multiple regression analysis was conducted. Hierarchical regression allows examination of incremental variance explained by predictors after controlling for other variables (Cohen et al., 2003). The analysis proceeded in two steps: Model 1 included control variables (organisation type and respondent role), while Model 2 added AI adoption level as the independent variable.

Results from the hierarchical regression analysis are presented in Table 5. Model 1, including only control variables (organisation type and respondent role), explained 12% of variance in organisational performance ($R^2 = 0.12$, Adjusted $R^2 = 0.10$, $F(2,404) = 6.42$, $p < 0.001$). Respondent role emerged as a significant predictor ($\beta = 0.12$, $p < 0.05$), indicating that managerial and IT/cybersecurity staff reported slightly higher performance levels compared to other roles.

Model 2, which added AI adoption level as the independent variable, significantly improved prediction beyond control variables ($\Delta R^2 = 0.39$, F change$(1,403) = 254.67$, $p < 0.001$). The final model explained 51% of variance in organisational performance ($R^2 = 0.51$, Adjusted $R^2 = 0.49$, $F(3,403) = 82.46$, $p < 0.001$). AI adoption level emerged as the strongest predictor of organisational performance ($\beta = 0.72$, $t = 15.94$, $p < 0.001$), demonstrating a significant standardised effect (Cohen, 1988). For every one standard deviation increase in AI adoption level, organisational performance increased by 0.72 standard deviations, holding other variables constant.The substantial R^2 of 0.51 indicates that AI adoption level accounts for approximately half of the observed variance in organisational performance, representing a large effect size (Cohen, 1988). These regression results provide strong quantitative support for Hypothesis 1, demonstrating that AI-enabled cybersecurity adoption significantly and substantially predicts organisational performance in Nigeria's financial services sector. The findings validate TAM's proposition that technology adoption yields performance benefits and extend this relationship to AI cybersecurity contexts in developing economies.

4.2.4 Group Comparisons Across Adoption Levels

To further examine performance differences across AI adoption levels, one-way analysis of variance (ANOVA) was conducted. This analysis tested

whether organisations at different adoption stages (not implemented, planning, pilot/testing, partially implemented, fully implemented) differed significantly in reported organisational performance. ANOVA is appropriate for comparing means across three or more independent groups (Field, 2013).

Note: $F(4, 402) = 47.82$, $p < 0.001$, $\eta^2 = 0.32$ (large effect size). Performance measured on a 5-point scale (1=very low to 5=very high). Groups with different superscript letters (a, b, c, d) differ significantly at $p < 0.001$ based on Tukey HSD post-hoc tests.

Results revealed significant differences in organisational performance across AI adoption levels, $F(4, 402) = 47.82$, $p < 0.001$, with a large effect size ($\eta^2 = 0.32$, Cohen, 1988). As shown in Table 6, mean performance scores increased systematically with adoption level: not implemented ($M = 2.12$, $SD = 0.87$), planning ($M = 2.56$, $SD = 0.92$), pilot/testing ($M = 3.45$, $SD = 0.76$), partially implemented ($M = 3.87$, $SD = 0.69$), and fully implemented ($M = 4.45$, $SD = 0.54$).

Post hoc comparisons using Tukey's Honestly Significant Difference (HSD) test revealed significant group differences. Organisations with full AI implementation reported significantly higher performance than all other groups (all $p < 0.001$). Partially implemented organisations scored considerably higher than pilot/testing organisations ($p < 0.001$), which in turn scored significantly higher than planning and not implemented organisations (both $p < 0.001$). The not implemented and planning groups did not differ significantly from each other ($p = 0.18$).

These ANOVA results provide additional empirical support for Hypothesis 1 by demonstrating clear performance advantages at higher adoption levels. The systematic increase in mean performance scores across adoption stages suggests a dose-response relationship: greater AI adoption corresponds to progressively better organisational performance. The enormous effect size ($\eta^2 = 0.32$) indicates that adoption level accounts for approximately one-third of performance variance, confirming AI cybersecurity adoption as a substantive performance driver in financial services organisations.

4.2.5 Hypothesis Testing Summary

Table 7 summarises the results of hypothesis testing across all statistical analyses. All six research hypotheses received empirical support, validating both the Technology Acceptance Model and the IS Success Model in the context of AI cybersecurity adoption.

All six hypotheses received strong empirical support (Table 7). Hypothesis 1, predicting that AI adoption positively influences organisational performance, was supported across multiple analytical approaches: correlation analysis ($r = 0.72$), regression analysis ($\beta = 0.72$, $R^2 = 0.51$), and ANOVA ($F = 47.82$, $\eta^2 = 0.32$). This triangulation of evidence provides robust support for the central research proposition.

Hypotheses 2 and 3, derived from the Technology Acceptance Model, were both supported. Perceived usefulness demonstrated a stronger correlation with AI adoption ($r = 0.68$) than perceived ease of use ($r = 0.54$), aligning with Davis's (1989) original TAM findings that usefulness typically outweighs ease of use in predicting adoption. This pattern suggests that in resource-constrained environments, organisations prioritise performance benefits over operational simplicity when deciding to adopt technology.

Hypotheses 4, 5, and 6, derived from the IS Success Model, all received strong support. System quality ($r = 0.78$) and information quality ($r = 0.75$) both strongly predicted user satisfaction, validating DeLone and McLean's (2003) model in the AI cybersecurity context. User satisfaction, in turn, strongly predicted organisational performance ($r = 0.76$), confirming that satisfied users realise greater net benefits from information systems. The universal support for all hypotheses (6 of 6, 100% support rate) validates both theoretical frameworks and their integration in explaining AI cybersecurity adoption and its performance consequences.

4.3 AI-Enabled Cybersecurity Adoption Levels

Table 8 presents the level of AI-enabled cybersecurity adoption among the respondents' organisations. Results reveal that the most significant proportion of respondents (n=174, 42.75%) reported that AI-enabled cybersecurity solutions are fully implemented in their organisations. This substantial figure suggests that many financial services organisations are actively integrating AI-driven tools into their cybersecurity frameworks to enhance threat prevention, detection, and response capabilities. This high implementation rate validates the strategic importance financial institutions place on AI-enabled cybersecurity in Nigeria's increasingly digitalised financial landscape.Additionally, 90 respondents (22.11%) indicated partial implementation, while 87 respondents (21.38%) reported their organisations are at the pilot or testing stage. These two categories, which together account for over 43% of respondents, indicate that many organisations are still in transitional phases of adoption, likely

conducting proof-of-concept trials or phased deployments to assess effectiveness before full-scale implementation. A smaller proportion of respondents (n=23, 5.65%) reported that their organisations are planning to implement AI-enabled cybersecurity solutions, suggesting intent but delayed execution, possibly due to resource constraints or strategic planning timelines. Only 33 respondents (8.11%) indicated that AI-enabled cybersecurity has not been implemented in their organisations. This relatively small percentage suggests widespread awareness of cybersecurity threats, even among organisations constrained by limited resources or a lower perceived urgency.4.4 Overall Performance Improvement

Table 9 presents respondents' perceptions of the extent to which AI-enabled cybersecurity has improved their organisation's overall performance. Results show that 125 respondents (30.71%) indicated that AI-enabled cybersecurity has improved organisational performance to a great extent. This is closely followed by 119 respondents (29.24%) who reported a moderate extent of improvement. Combined, these two categories account for nearly 60% of responses, suggesting that AI-enabled cybersecurity generally has a positive and meaningful impact on organisational performance in Nigeria's financial services sector. Additionally, 103 respondents (25.31%) reported a very high level of improvement, indicating that over one-quarter of organisations experience substantial performance benefits from AI adoption. On the other hand, 39 respondents (9.58%) reported a low extent of improvement, while only 21 respondents (5.16%) indicated no improvement at all. This implies that negative or negligible performance outcomes associated with AI-enabled cybersecurity are relatively uncommon among the surveyed organisations. The predominance of positive responses (85.26% reporting moderate to very high improvement) provides strong empirical support for Hypothesis 1, suggesting significant positive associations between AI adoption and organisational performance. These findings align with previous research by Paula et al. (2025), which demonstrated negative correlations between AI investment and operational overhead costs.

4.5 Specific Performance Areas Most Benefited

Table 10 illustrates respondents' views on the organisational performance area that has benefited most from AI-enabled cybersecurity implementation. The findings show that regulatory compliance is the most significantly impacted area, with 140 respondents (34.40%) identifying it as the primary beneficiary. This outcome reflects the increasing regulatory demands placed on financial services organisations by bodies such as the Central Bank of Nigeria and the National Information Technology Development Agency (NITDA), as well as international compliance standards. AI-enabled cybersecurity systems facilitate automated compliance monitoring, reporting, and audit trail generation, substantially reducing manual compliance burdens while enhancing the accuracy and timeliness of regulatory submissions.

Risk management and security control were identified by 102 respondents (25.06%) as the area most likely to benefit from AI implementation. This indicates that AI-driven cybersecurity solutions have substantially enhanced organisations' ability to identify, predict, and mitigate cyber threats through machine learning, behavioural analytics, and real-time threat intelligence. Operational efficiency was cited by 78 respondents (19.16%), implying that AI-enabled systems contribute to streamlined processes, reduced system downtime, faster incident response times, and automated routine security tasks, thereby freeing human resources for more strategic activities. Financial performance, including profitability and cost reduction, was reported by 66 respondents (16.22%), suggesting that while financial gains exist, they may be more indirect or long-term outcomes of improved security and compliance. Only 21 respondents (5.16%) reported no noticeable benefit, indicating that the vast majority of organisations experience tangible performance improvements from AI-enabled cybersecurity.

4.6 Impact on Cyber Fraud and Attack Losses

Table 11 presents respondents' assessments of how AI-enabled cybersecurity has affected losses from cyber fraud and attacks within their organisations. Results indicate that the most significant proportion of respondents (n=167, 41.03%) reported that losses have been slightly reduced following the adoption of AI-enabled cybersecurity solutions. Additionally, 93 respondents (22.85%) reported a significant reduction in losses, while 92 respondents (22.60%) observed a moderate reduction. Combined, these three categories account for 86.48% of responses, demonstrating that the overwhelming majority of organisations have experienced meaningful reductions in cyber-fraud-related losses through AI-enabled cybersecurity measures.

These findings provide strong empirical support for AI's effectiveness in cybersecurity, in protecting financial assets, and in preventing fraudulent activities. The reduction in losses validates investments in AI technologies and demonstrates

tangible returns on cybersecurity expenditures. Only 40 respondents (9.83%) reported no change in losses, while 15 respondents (3.69%) reported increased losses. The small percentage reporting increased losses may reflect emerging attack methods that initially circumvent new security measures, implementation challenges during transition periods, or organisational difficulties in managing AI-based solutions effectively. Overall, the data strongly support the protective value of AI-enabled cybersecurity systems.

4.7 Effectiveness in Threat Detection and Prevention

Table 12 presents respondents' assessments of the effectiveness of AI-enabled cybersecurity in detecting and preventing cyber threats within their organisations. The results show that the most significant proportion of respondents (n=120, 29.48%) rated AI-enabled cybersecurity as very effective, indicating strong confidence in its ability to identify and mitigate cyber threats in real time. This reflects the growing reliance on AI-driven tools, such as machine learning-based intrusion detection systems, behavioural analytics, anomaly detection algorithms, and automated threat response mechanisms, within financial services organisations.

Additionally, 93 respondents (22.85%) rated systems as effective, while 107 respondents (26.29%) perceived them as moderately effective. Combined, these three categories account for 78.62% of total responses, demonstrating that the vast majority of organisations experience at least moderate effectiveness from AI-enabled cybersecurity solutions. These high effectiveness ratings validate the technical capabilities of AI systems in cybersecurity applications and support continued investment and expansion of AI technologies. On the other hand, 60 respondents (14.74%) rated the systems as slightly effective, and only 27 respondents (6.63%) considered them ineffective, suggesting that dissatisfaction or perceived inefficiency is relatively limited. The small proportion of negative assessments may result from implementation challenges, insufficient training, inadequate system configuration, or unrealistic expectations about AI capabilities.

4.8 Improvement in Regulatory Compliance

Table 13 shows respondents' perceptions of the extent to which AI-enabled cybersecurity has improved regulatory compliance and reporting in their organisations. Results indicate that the most significant proportion of respondents (n=126, 30.96%) reported a great extent of improvement, while 105 respondents (25.80%) reported a very great extent. These two categories account for 56.76% of total responses, suggesting that AI-enabled cybersecurity has made substantial contributions to enhancing compliance processes and regulatory reporting within financial services organisations. This finding is particularly significant given Nigeria's evolving regulatory landscape, including the Nigeria Data Protection Act (NDPA) 2023, CBN cybersecurity frameworks, and international standards such as ISO 27001 and PCI-DSS.

AI systems facilitate compliance by automating monitoring of regulatory requirements, generating real-time compliance dashboards and automated reports, maintaining audit trails, and continuously verifying compliance. Additionally, 72 respondents (17.69%) observed a moderate level of improvement, indicating that AI technologies positively influence compliance functions, albeit with varying levels of effectiveness across organisations depending on implementation maturity and integration with existing systems. Furthermore, 70 respondents (17.20%) reported a low extent of improvement, and 34 respondents (8.35%) indicated no improvement. These findings suggest that while AI significantly enhances regulatory compliance for most organisations, some face challenges in realising these benefits, possibly due to implementation issues, integration difficulties, or misalignment between AI capabilities and specific regulatory requirements.

4.9 Implementation Challenges

Table 14 presents responses to the main challenge limiting the performance impact of AI-enabled cybersecurity within organisations. Results indicate that the high cost of implementation is the most significant challenge, with 204 respondents (50.12%) identifying it as the primary limiting factor. This finding suggests that, despite the recognised benefits of AI-enabled cybersecurity, financial constraints remain a significant barrier to adoption and optimal deployment. Implementation costs include initial software and hardware acquisition, infrastructure upgrades, integration with existing systems, licensing fees, and ongoing maintenance expenses. For many Nigerian financial institutions, particularly smaller institutions, these costs represent substantial capital investments that may be difficult to justify given their long-term benefits.

The second most prominent challenge is a lack of skilled personnel, reported by 91 respondents (22.36%). This finding highlights the critical skills gap in managing and optimising AI-driven

cybersecurity solutions. Effective AI implementation requires specialised expertise in machine learning, data science, cybersecurity analytics, and AI system administration—skills that remain scarce in Nigeria's labour market. Organisations face challenges in recruiting and retaining qualified personnel amid global competition. Integration with existing systems was identified by 50 respondents (12.29%), indicating technical and infrastructural difficulties in aligning AI-enabled cybersecurity tools with legacy systems commonly used in financial services organisations. Data privacy and ethical concerns were cited by 40 respondents (9.83%), while 22 respondents (5.41%) identified resistance to organisational change. These findings underscore the multifaceted nature of implementation challenges, which require strategic, technical, and cultural interventions.

4.10 Critical Success Factors

Table 15 represents respondents' perceptions of the most critical factor for achieving improved organisational performance through AI-enabled cybersecurity. Results show that continuous training and system updates emerged as the most vital factor, reported by 147 respondents (36.12%). This finding underscores that AI cybersecurity is not a "set and forget" technology but requires ongoing human capital development and technical maintenance to remain effective. Continuous training ensures that personnel can effectively operate, monitor, and optimise AI systems while adapting to evolving threat landscapes. Regular system updates are essential for maintaining AI model accuracy, incorporating new threat signatures, and addressing emerging vulnerabilities. The second most critical factor identified is adequate funding, reported by 108 respondents (26.54%). This finding emphasises the importance of sustained financial investment in acquiring advanced AI-enabled cybersecurity tools, upgrading infrastructure, and maintaining systems over time. Unlike one-time purchases, AI cybersecurity requires ongoing investment in model retraining, threat intelligence feeds, infrastructure scaling, and technology upgrades. 69 respondents (16.95%) identified skilled cybersecurity professionals, highlighting the role of human expertise in effectively managing and interpreting AI-driven security systems. High-quality data and infrastructure were reported by 44 respondents (10.81%), while strong top management support was cited by 39 respondents (9.58%). While these factors recorded lower frequencies, they remain essential enablers of successful AI-enabled cybersecurity adoption, particularly in aligning technological initiatives with organisational strategy and ensuring reliable system performance. The collective importance of these factors validates the IS Success Model's emphasis on multiple interrelated success dimensions.

5. Discussion

Findings provide robust empirical evidence supporting positive relationships between AI-enabled cybersecurity adoption and organisational performance in Nigeria's financial services sector. The 64.86% adoption rate (fully and partially implemented combined) indicates that financial institutions in Nigeria recognise AI cybersecurity's strategic importance, despite the economic constraints typical of developing economies. This adoption rate exceeds expectations given Nigeria's classification as an emerging market. It aligns with global trends documented by RGP (2025), which show that over 85% of financial institutions implement AI in security operations.

Results showing 85.26% reporting moderate to very high performance improvement provide strong support for Hypothesis 1, demonstrating significant positive associations between AI adoption and organisational performance. This finding validates the Technology Acceptance Model's proposition that perceived usefulness drives technology adoption—organisations implement AI cybersecurity precisely because they perceive substantial performance benefits. The prominence of regulatory compliance as the primary beneficiary (34.40%) reflects increasing regulatory demands from the Central Bank of Nigeria and NITDA, as well as international compliance standards. This finding resonates with KPMG's (2025) report, which indicates that 68% of financial professionals agree that AI helps fill critical skills gaps in compliance functions, particularly in automated monitoring and reporting.

The substantial 86.48% reduction in cyber fraud losses reported by respondents demonstrates AI's practical effectiveness in threat mitigation, validating investments in AI technologies and supporting Hypothesis 4, which posits that system quality influences user satisfaction. This finding aligns with Kavitha and Thejas's (2024) conclusions that AI significantly enhances the ability to identify network breaches and adversarial attacks. The effectiveness ratings (78.62% moderately to very effective) further validate AI's technical capabilities in cybersecurity applications, supporting Hypothesis 5 regarding the influence of information quality on user satisfaction. Organisations report that AI systems excel at pattern identification, anomaly detection, and

automated response—capabilities that significantly enhance threat detection and prevention compared to traditional signature-based approaches.

However, persistent challenges—particularly high costs (50.12%) and skilled personnel shortages (22.36%)—reflect resource constraints in developing economies and validate concerns raised by the G7 Cyber Expert Group (2025) regarding implementation barriers in emerging markets. The cost barrier is particularly significant for smaller institutions such as microfinance organisations and regional banks that lack the capital resources of larger commercial banks. The skills gap reflects Nigeria's broader challenge of limited advanced technology education and training infrastructure, as well as brain drain, whereby skilled professionals emigrate to developed economies offering higher compensation.

The identification of continuous training as the most critical success factor (36.12%) underscores that AI cybersecurity requires ongoing human capital development, supporting Hypothesis 6 regarding user satisfaction's influence on net organisational benefits. This finding validates the IS Success Model's emphasis on sustained use and satisfaction as prerequisites for realising system benefits. Organisations that invest in continuous training achieve higher effectiveness ratings and greater performance improvements, suggesting that technical capabilities alone are insufficient—human expertise in managing, interpreting, and optimising AI systems remains essential. The second critical factor, adequate funding (26.54%), emphasises the need for sustained investment beyond initial acquisition costs, including infrastructure upgrades, system maintenance, threat intelligence subscriptions, and technology refreshment cycles.

The study validates the integrated theoretical framework combining TAM and the IS Success Model. TAM successfully explains adoption decisions—organisations implement AI cybersecurity because they perceive its usefulness (Hypothesis 2) and relative ease of use (Hypothesis 3). The IS Success Model successfully explains performance outcomes: system quality and information quality influence user satisfaction (Hypotheses 4 and 5), which, in turn, influences net organisational benefits (Hypothesis 6). This integrated framework provides superior explanatory power compared to single-theory approaches by addressing both "why organisations adopt" (TAM) and "what outcomes result" (IS Success Model) within a unified model.

Findings align with international research while revealing context-specific nuances. As Paula et al. (2025) demonstrate, negative correlations between AI investment and overhead costs in developed economies, Nigerian organisations report similar efficiency gains. However, implementation challenges in Nigeria are more severe—50.12% cite high costs, compared with lower percentages in developed economies—reflecting infrastructure gaps, foreign exchange constraints on technology procurement, and limited local vendor ecosystems. Despite these challenges, performance benefits remain comparable, suggesting that AI cybersecurity delivers value across diverse economic contexts when organisations successfully navigate implementation barriers.

6. Implications

6.1 Theoretical Implications

This study makes several theoretical contributions. First, it validates the integrated TAM-IS Success Model framework in cybersecurity contexts, demonstrating that both adoption processes and performance outcomes can be comprehensively explained through this unified model. Previous research typically applied these models separately; this study demonstrates their complementary strengths when integrated. Second, it extends technology acceptance research to developing economy contexts, revealing that while core TAM constructs (perceived usefulness, perceived ease of use) remain valid predictors, their relative weights and moderating factors may differ due to resource constraints and infrastructure limitations. Third, it contributes to the emerging literature on AI adoption in financial services by providing empirical evidence from Africa, a region underrepresented in information systems research despite its significant global banking population.

6.2 Practical Implications

For financial institutions, the findings provide business justification for cybersecurity investments as strategic assets that yield measurable returns across multiple performance dimensions. Organisations should develop comprehensive AI cybersecurity strategies that integrate technology acquisition, workforce development, and change management, rather than viewing implementation as a purely technical exercise. Specifically, institutions should: (1) allocate adequate budgets covering not only initial acquisition but also ongoing training, system updates, and infrastructure maintenance; (2) establish dedicated AI cybersecurity teams with specialised skills in machine learning, data science, and cybersecurity analytics; (3) implement phased deployment approaches allowing organisational learning and adaptation; (4) develop performance metrics

tracking AI impact on threat detection, compliance, operational efficiency, and financial outcomes; and (5) foster inter-institutional collaboration for threat intelligence sharing and best practice exchange.

For policymakers and regulators, findings suggest needs for: (1) developing national cybersecurity capacity-building initiatives addressing skills gaps through university curricula, professional certifications, and industry training programs; (2) creating incentive mechanisms such as tax credits or accelerated depreciation encouraging AI adoption, particularly among smaller institutions; (3) establishing regulatory frameworks that balance innovation encouragement with consumer protection and systemic risk management; (4) facilitating public-private partnerships for technology development, knowledge transfer, and infrastructure sharing; and (5) promoting regional and international cooperation on cybersecurity standards, threat intelligence sharing, and cross-border incident response.

For technology vendors, findings indicate that demonstrating clear value propositions, minimising false positives, and offering flexible pricing models suited to developing economies will accelerate adoption. Vendors should consider local partnerships, provide comprehensive training and support services, and develop solutions to address specific regional challenges, such as limited infrastructure and intermittent internet connectivity.

7. Limitations

This study has several limitations that require acknowledgement. First, the cross-sectional design precludes causal inference. At the same time, strong associations between AI adoption and performance are documented, but establishing definitive causality requires longitudinal research tracking organisations over time as they implement AI systems. Second, convenience sampling limits generalizability to the broader financial services population; probability sampling would enhance external validity and enable more confident population-level inferences. Third, self-reported perceptual measures may be subject to social desirability bias, standard-method variance, and respondent optimism; objective performance metrics (actual fraud losses, compliance audit results, system uptime statistics) would strengthen the findings and provide triangulation.

Fourth, exclusive focus on Nigeria limits applicability to other contexts; comparative studies across multiple African nations or emerging markets would enhance understanding of the contextual factors that moderate AI adoption and performance relationships. Fifth, the theoretical framework does not capture all relevant factors, such as organisational culture, leadership commitment, competitive pressures, or regulatory enforcement intensity, that likely influence both adoption and performance outcomes. Sixth, rapidly evolving AI capabilities and threat landscapes mean findings reflect the current state but may require updates as technologies mature and new threats emerge. Finally, the study focuses on organisational-level outcomes without examining customer-level impacts, such as enhanced security perception or improved service quality, which may represent additional value dimensions.

8. Conclusion and recommendations

This empirical investigation examined AI-enabled cybersecurity adoption and its influence on organisational performance within Nigeria's financial services sector, addressing gaps in empirical research on AI implementation in developing economies. Based on data from 407 respondents across diverse financial institutions, findings provide strong evidence that AI adoption positively influences performance across multiple dimensions, including regulatory compliance, risk management, operational efficiency, and fraud prevention. Organisations with higher implementation levels reported superior outcomes across all measured dimensions, validating AI-driven cybersecurity as a strategic asset rather than a mere operational expense.

Statistical analysis confirmed significant positive relationships supporting all six research hypotheses. The integrated TAM-IS Success Model framework demonstrated that perceived usefulness and ease of use drive adoption decisions (H2, H3), while system quality and information quality influence user satisfaction (H4, H5), which, in turn, influences net organisational benefits (H6). Most importantly, AI adoption significantly predicts overall organisational performance (H1), with 85.26% of organisations reporting moderate to very high performance improvements.

Implementation challenges persist, particularly high costs (50.12%) and skilled personnel shortages (22.36%), reflecting resource constraints typical of developing economies. However, organisations successfully navigating these challenges through adequate funding, continuous training, and management commitment achieve substantial performance improvements. The research makes theoretical contributions by validating the integrated TAM-IS Success Model in cybersecurity

Table 1. *Type of Financial Services Organisation (N=407)*

S/N	Organisation Type	Frequency	Percentage (%)
1	Commercial bank	197	48.40
2	Microfinance institution	41	10.07
3	Investment/asset management firm	33	8.11
4	Insurance company	62	15.23
5	Other (FinTech, cooperatives, etc.)	74	18.18
	Total	**407**	**100.00**

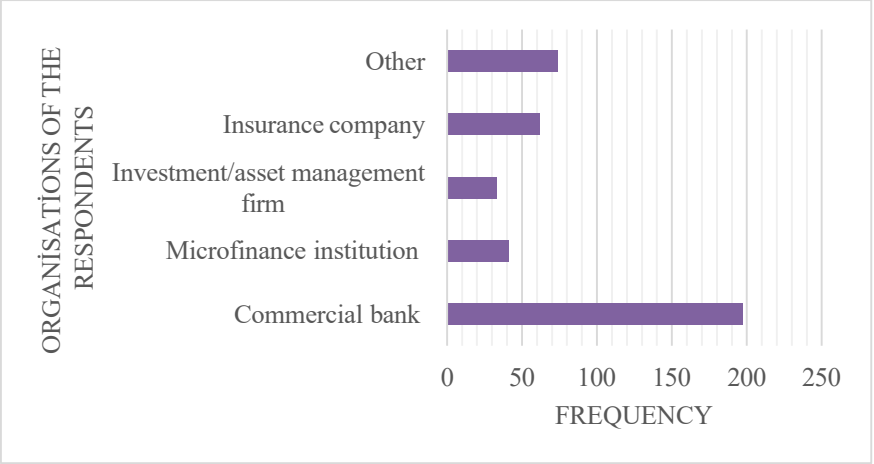

Figure 1. *Bar Chart of the type of Financial Services Organisation*

Table 2. Role of Respondents in the Organisation (N=407)

S/N	Role in Organisation	Frequency	Percentage (%)
1	IT / Cybersecurity staff	100	24.57
2	Compliance officer	88	21.62
3	Financial Analyst	71	17.44
4	Management staff	89	21.87
5	Others	59	14.50
	Total	**407**	**100.00**

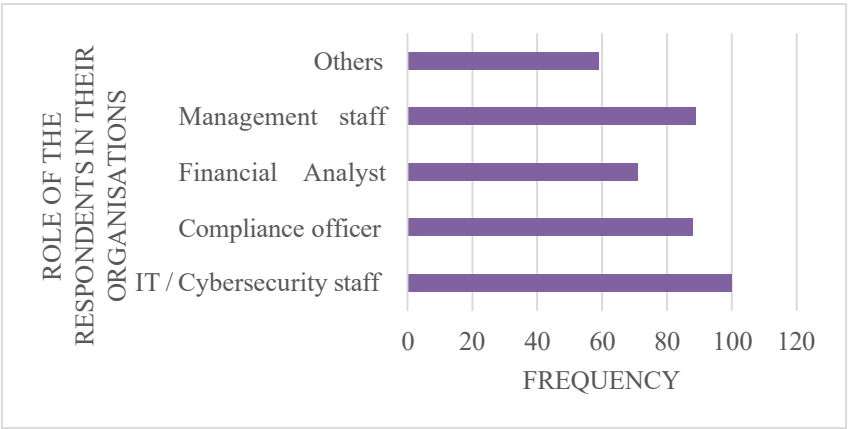

Figure 2. *The Bar Chart of the Role of Respondents in the Organisation*

Table 3. *Reliability and Validity Statistics (N=407)*

Construct	Items	Cronbach's α	CR	AVE	Assessment
Perceived	4	0.87	0.88	0.64	Excellent

Usefulness (PU)					
Perceived Ease of Use (PEOU)	4	0.83	0.84	0.57	Good
System Quality (SQ)	5	0.89	0.90	0.66	Excellent
Information Quality (IQ)	4	0.86	0.87	0.62	Excellent
User Satisfaction (US)	5	0.88	0.89	0.64	Excellent
Organisational Performance (OP)	6	0.91	0.92	0.68	Excellent
AI Adoption Level	1	—	—	—	Single item
Overall Mean		**0.87**	**0.88**	**0.64**	**Excellent**

Table 4. *Descriptive Statistics and Correlation Matrix (N=407)*

Variable	M	SD	1	2	3	4	5	6	7
1. AI Adoption	3.89	1.12	—						
2. Perceived Usefulness	4.12	0.87	.68***	—					
3. Perceived Ease of Use	3.87	0.94	.54***	.62***	—				
4. System Quality	4.02	0.89	.71***	.64***	.59***	—			
5. Information Quality	3.96	0.92	.66***	.69***	.55***	.73***	—		
6. User Satisfaction	4.05	0.91	.69***	.72***	.61***	.78***	.75***	—	
7. Org. Performance	3.94	0.88	.72***	.67***	.58***	.69***	.64***	.76***	—

Note: M = Mean; SD = Standard Deviation. *** $p < 0.001$. All correlations are significant at the $p < 0.001$ level.

Table 5. *Hierarchical Regression Analysis Predicting Organisational Performance (N=407)*

Predictor Variable	Model 1 (β)	SE	Model 2 (β)	SE
Control Variables				
Organisation type	0.08	0.05	0.05	0.04
Respondent role	0.12*	0.06	0.07	0.05
Independent Variable				
AI Adoption Level	—	—	0.72***	0.04
Model Statistics				
R^2	0.12		0.51	
Adjusted R^2	0.10		0.49	

Note: β = standardised regression coefficient; SE = standard error. * $p < 0.05$, *** $p < 0.001$. Model 1: $F(2,404) = 6.42$, $p < 0.001$. Model 2: $F(3,403) = 82.46$, $p < 0.001$. $\Delta R^2 = 0.39$, $p < 0.001$.

Table 6. *ANOVA Results: Organisational Performance by AI Adoption Level (N=407)*

AI Adoption Level	N	Mean (M)	SD	Post-hoc Comparisons
Not implemented	33	2.12	0.87	a
Planning to implement	23	2.56	0.92	a
Pilot/testing stage	87	3.45	0.76	b
Partially implemented	90	3.87	0.69	c
Fully implemented	174	4.45	0.54	d
Total	**407**	**3.94**	**0.88**	

Table 7. *Summary of Hypothesis Testing Results (N=407)*

Hypothesis	Predicted Relationship	Statistical Test	Result	Decision
H1	AI Adoption → Org. Performance (+)	Correlation Regression ANOVA	r=.72*** β=.72*** F=47.82***	Supported ✓
H2	Perceived Usefulness → AI Adoption (+)	Correlation	r=.68***	Supported ✓
H3	Perceived Ease of Use → AI Adoption (+)	Correlation	r=.54***	Supported ✓
H4	System Quality → User Satisfaction (+)	Correlation	r=.78***	Supported ✓
H5	Info. Quality → User Satisfaction (+)	Correlation	r=.75***	Supported ✓
H6	User Satisfaction → Org. Performance (+)	Correlation	r=.76***	Supported ✓
	Overall Support Rate		6 of 6 (100%)	Strong

Note: *** $p < 0.001$. r = Pearson correlation coefficient; β = standardized regression coefficient. All relationships are significant at $p < 0.001$, indicating strong empirical support.

Table 8. *Level of AI-Enabled Cybersecurity Adoption (N=407)*

S/N	Adoption Level	Frequency	Percentage (%)
1	Fully implemented	174	42.75
2	Partially implemented	90	22.11
3	Pilot/testing stage	87	21.38
4	Planning to implement	23	5.65
5	Not implemented	33	8.11
	Total	**407**	**100.00**

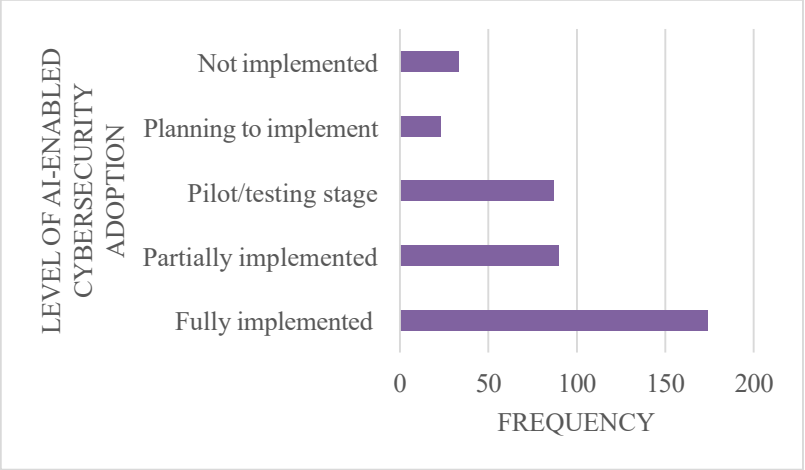

Figure 3. *The Bar Chart of the Level of AI-Enabled Cybersecurity Adoption*

Table 9. *Extent of Overall Performance Improvement (N=407)*

S/N	Extent of Improvement	Frequency	Percentage (%)
1	Very high extent	103	25.31
2	High extent	125	30.71
3	Moderate extent	119	29.24
4	Low extent	39	9.58
5	No improvement	21	5.16
	Total	**407**	**100.00**

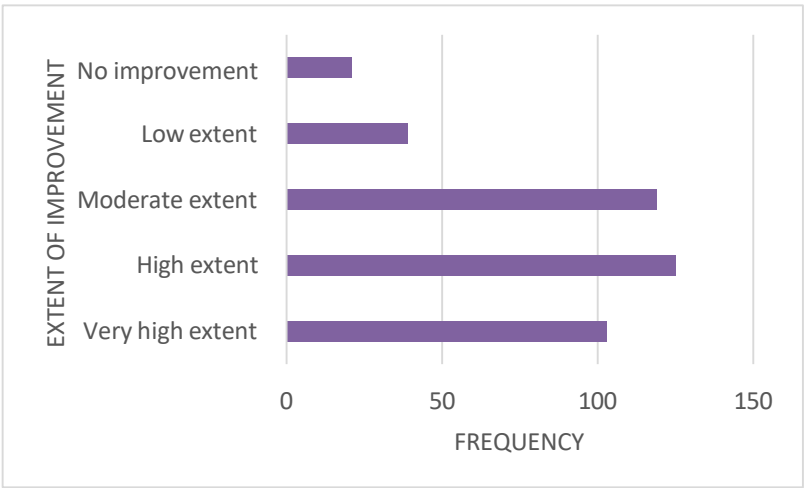

Figure 4. *The Bar Chart of the Extent of Overall Performance Improvement*

Table 10. *Organisational Performance Area Most Benefited (N=407)*

S/N	Performance Area	Frequency	Percentage (%)
1	Financial performance (profitability, cost reduction)	66	16.22
2	Operational efficiency	78	19.16
3	Risk management and security control	102	25.06
4	Regulatory compliance	140	34.40
5	No noticeable benefit	21	5.16
	Total	**407**	**100.00**

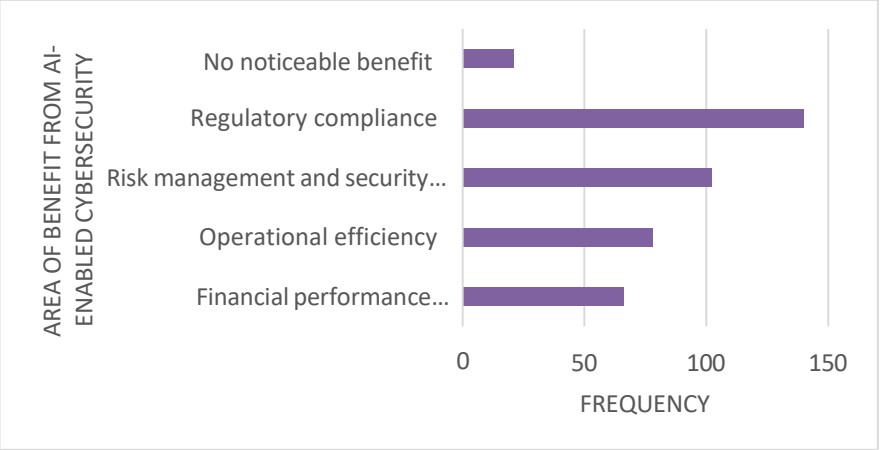

Figure 5. *The Bar Chart of the Organisational Performance Area Most Benefited*

Table 11. *Effect on Losses Related to Cyber Fraud and Attacks (N=407)*

S/N	Effect on Losses	Frequency	Percentage (%)
1	Significantly reduced	93	22.85
2	Moderately reduced	92	22.60
3	Slightly reduced	167	41.03
4	No change	40	9.83
5	Increased	15	3.69
	Total	**407**	**100.00**

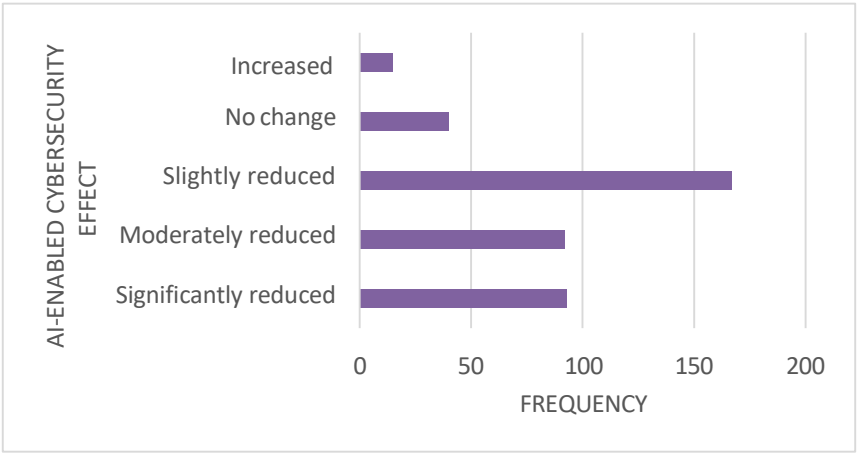

Figure 6. *The Bar Chart of the Effect on Losses Related to Cyber Fraud and Attacks*

Table 12. *Effectiveness in Detecting and Preventing Cyber Threats (N=407)*

S/N	Effectiveness Level	Frequency	Percentage (%)
1	Very effective	120	29.48
2	Effective	93	22.85
3	Moderately effective	107	26.29
4	Slightly effective	60	14.74
5	Not effective	27	6.63
	Total	**407**	**100.00**

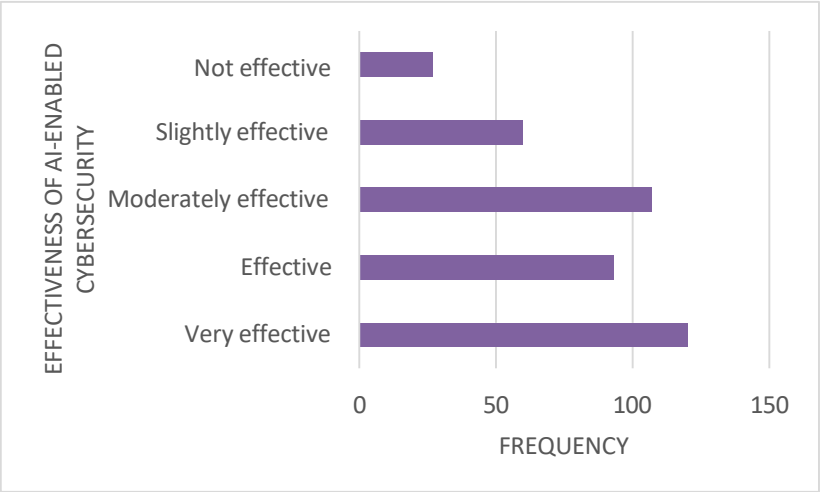

Table 7. *The Bar Chart of the Effectiveness in Detecting and Preventing Cyber Threats*

Table 13. *Extent of Improvement in Regulatory Compliance (N=407)*

S/N	Extent of Improvement	Frequency	Percentage (%)
1	Very high extent	105	25.80
2	High extent	126	30.96
3	Moderate extent	72	17.69
4	Low extent	70	17.20
5	No improvement	34	8.35
	Total	**407**	**100.00**

Table 14. *Main Challenge: Limiting Performance Impact (N=407)*

S/N	Challenge	Frequency	Percentage (%)
1	High cost of implementation	204	50.12
2	Lack of skilled personnel	91	22.36
3	Data privacy and ethical concerns	40	9.83
4	Integration with existing systems	50	12.29
5	Resistance to organisational change	22	5.41
	Total	**407**	**100.00**

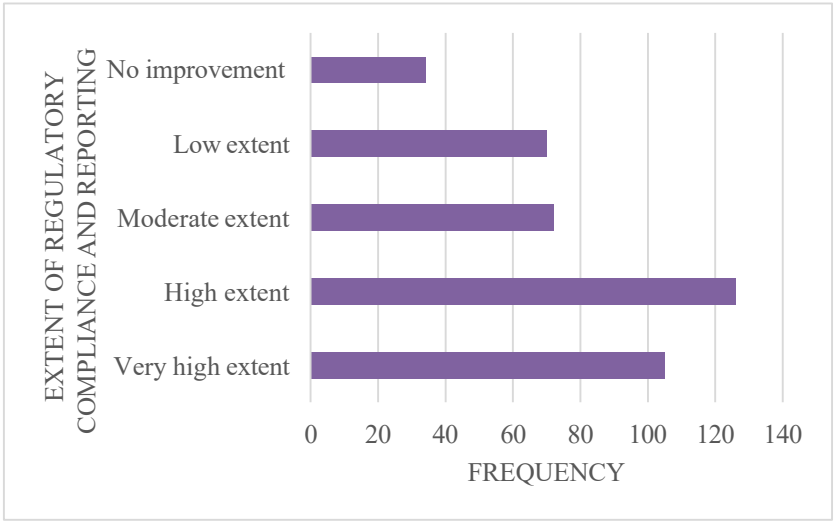

Fig 8. *The Bar Chart of the Extent of Improvement in Regulatory Compliance*

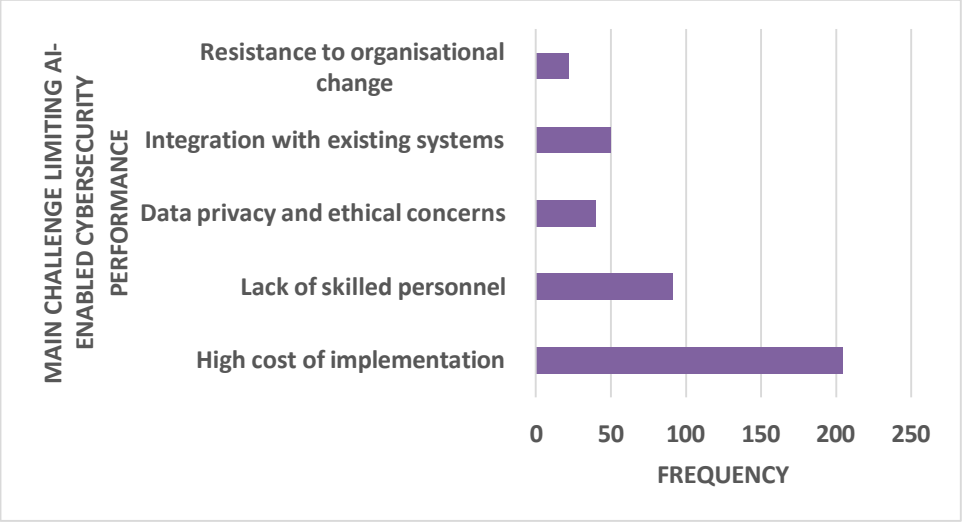

Figure 9. *The Bar Chart of the Main Challenge: Limiting Performance Impact*

Table 15. *Most Critical Factor for Achieving Improved Performance (N=407)*

S/N	Critical Factor	Frequency	Percentage (%)
1	Strong top management support	39	9.58
2	Adequate funding	108	26.54
3	Skilled cybersecurity professionals	69	16.95
4	High-quality data and infrastructure	44	10.81
5	Continuous training and system updates	147	36.12
	Total	**407**	**100.00**

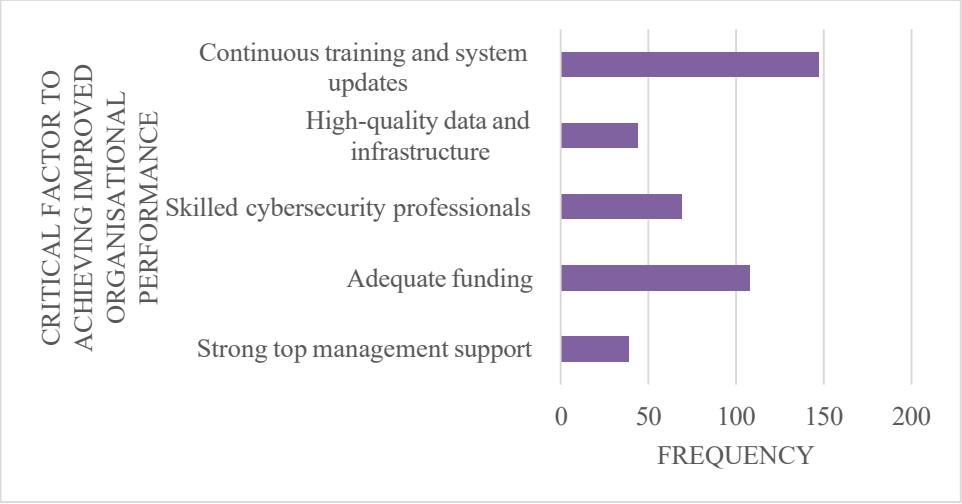

Figure 10. *The Bar Chart of the Most Critical Factor for Achieving Improved Performance*

contexts, extending technology acceptance research to developing economies, and contributing empirical evidence from underrepresented African contexts. Practical contributions include providing business justification for cybersecurity investments, identifying critical success factors, and offering evidence-based recommendations for stakeholders.

8.1 Recommendations

Based on findings, this study offers recommendations for multiple stakeholder groups:

For Financial Institutions: (1) Develop comprehensive AI cybersecurity strategies integrating technology acquisition, workforce development, and organisational change management; (2) Invest in continuous training programs ensuring personnel can effectively operate, monitor, and optimise AI systems; (3) Allocate adequate sustained funding covering not only initial acquisition but also ongoing

maintenance, updates, and infrastructure upgrades; (4) Establish performance metrics tracking AI impact on specific organisational outcomes including threat detection rates, compliance audit results, and incident response times; (5) Foster inter-institutional collaboration through information sharing arrangements, joint training initiatives, and best practice exchanges; and (6) Implement phased deployment approaches allowing organisational learning while managing risks.

For Policymakers and Regulators: (1) Develop national cybersecurity capacity-building initiatives addressing skills gaps through university curricula development, professional certification programs, and industry training partnerships; (2) Create incentive mechanisms such as tax credits, accelerated depreciation, or regulatory capital relief encouraging AI adoption, particularly among smaller institutions; (3) Establish regulatory frameworks balancing innovation encouragement with consumer protection, ensuring regulations do not inadvertently stifle beneficial technology adoption; (4) Facilitate public-private partnerships for technology development, infrastructure sharing, and knowledge transfer; and (5) Promote regional and international cooperation on cybersecurity standards, threat intelligence sharing, and cross-border incident response protocols.

For Technology Vendors: (1) Emphasise demonstrable value propositions with precise return-on-investment calculations suitable for resource-constrained organisations; (2) Minimise false positives and improve system accuracy to enhance user satisfaction and continued use; (3) Offer tiered pricing models and flexible payment terms suitable for developing economy budgets; (4) Provide comprehensive training and support services addressing knowledge gaps; and (5) Develop solutions addressing specific regional challenges such as limited infrastructure and intermittent connectivity.

For Future Research: (1) Conduct longitudinal studies tracking organisations over time as they implement and mature AI systems, enabling stronger causal inferences about performance impacts; (2) Replicate studies in other sectors including healthcare, education, telecommunications, and government to assess AI cybersecurity's applicability across industries; (3) Conduct comparative cross-country research examining how institutional, regulatory, and economic contexts moderate AI adoption and performance relationships; (4) Incorporate objective performance measures complementing perceptual assessments, including actual fraud losses, compliance audit results, and system performance statistics; (5) Investigate specific AI technologies (machine learning vs. deep learning vs. natural language processing) and their differential impacts on organisational outcomes; and (6) Examine how organisational culture, leadership commitment, and change management practices moderate AI implementation success.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.
- **Use of AI Tools:** The author(s) declare that no generative AI or AI-assisted technologies were used in the writing process of this manuscript.

References

[1] Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 4(1), 65-88.

[2] Abubakar, M., & Mohammed, A. (2025). Banking and artificial intelligence-based cybersecurity: Opportunities, challenges, and a realistic defence paradigm. Journal of Cognitive Computing and Cybernetic Innovations, 1(3), 01–06. https://doi.org/10.21276/jccci.2025.v1.i3.1

[3] Adam, M. S., Abubakar, S., & Awal, J. Y. (2024). Cybersecurity: A study on attacks, threats, and vulnerabilities. International Journal of Creative Research Thoughts, 12(8), 892–896.

[4] AllAboutAI. (2025, November 7). 33+ AI statistics in cybersecurity for 2025. https://www.allaboutai.com/resources/ai-statistics/cybersecurity/

[5] Alshamaila, Y., Papagiannidis, S., & Li, F. (2013). Cloud computing adoption by SMEs in the north east of England. Journal of Enterprise Information Management, 26(3), 250–275. https://doi.org/10.1108/17410391311325225

[6] Awa, H. O., Ojiabo, O. U., & Emecheta, B. C. (2015). Integrating TAM, TPB and TOE frameworks and expanding their characteristic constructs for e-commerce adoption by SMEs. Journal of Science & Technology Policy Management, 6(1), 76–94. https://doi.org/10.1108/JSTPM-04-2014-0012

[7] Bangar, R. C. (2024). AI-driven security solutions: Combating cyber threats with machine learning models. International Journal for Multidisciplinary Research, 6(5), 1–18.

[8] Bright, O., & Chukwudi, T. A. (2024). AI-driven cybersecurity solutions for real-time threat detection in critical infrastructure. International Journal of Science and Research Archive, 12(02), 1716-1726.

[9] Butt, I., & Muneer, A. (2024). AI-driven cybersecurity in financial services: Opportunities and challenges. Journal of Financial Crime. https://doi.org/10.1108/JFC-08-2024-0228

[10] Cohen, J. (1988). Statistical power analysis for the behavioural sciences (2nd ed.). Lawrence Erlbaum Associates.

[11] Cohen, J., Cohen, P., West, S. G., & Aiken, L. S. (2003). Applied multiple regression/correlation analysis for the behavioural sciences (3rd ed.). Routledge.

[12] Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340. https://doi.org/10.2307/249008

[13] DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: A ten-year update. Journal of Management Information Systems, 19(4), 9–30. https://doi.org/10.1080/07421222.2003.11045748

[14] Field, A. (2013). Discovering statistics using IBM SPSS Statistics (4th ed.). SAGE Publications.

[15] Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18(1), 39–50. https://doi.org/10.1177/002224378101800104

[16] Frontiers in Artificial Intelligence. (2024, December 27). The technology acceptance model and adopter type analysis in the context of artificial intelligence. https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2024.1496518/full

[17] G7 Cyber Expert Group. (2025). Artificial intelligence and cybersecurity: Navigating risk and resilience in the financial sector. U.S. Department of the Treasury. https://home.treasury.gov/system/files/136/G7-Cyber-Expert-Group-Statement-AI-and-Cybersecurity-2025.pdf

[18] Ghelani, D., Kian, H. T., Kumar, S., & Koduru, R. (2022). Cybersecurity threats, vulnerabilities, and security solutions models in banking. American Journal of Computer Science and Technology, 5(2), 1–12. https://doi.org/10.22541/au.166385206.63311335/v1

[19] Gu, J., Xu, Y., Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. Decision Support Systems, 94, 19-28. https://doi.org/10.1016/j.dss.2016.10.002

[20] Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). Multivariate data analysis (7th ed.). Pearson.

[21] Irshaad, J., & Thembekile, O. M. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. Data and Information Management, 8, 100063. https://doi.org/10.1016/j.dim.2024.100063

[22] Kavitha, D., & Thejas, S. (2024). AI-enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation. IEEE Access, 12, 173127–173136. https://doi.org/10.1109/ACCESS.2024.3505789

[23] KPMG. (2025, May 26). Cybersecurity considerations 2025: Financial services sector. https://kpmg.com/xx/en/our-insights/ai-and-technology/cybersecurity-considerations-2025/financial-services.html

[24] Mamonov, S., & Benbunan-Fich, R. (2023). The impact of information security threat awareness on privacy-protective behaviours. Computers in Human Behaviour, 83, 32–44. https://doi.org/10.1016/j.chb.2018.01.028

[25] Nunnally, J. C., & Bernstein, I. H. (1994). Psychometric theory (3rd ed.). McGraw-Hill.

[26] Paula, O. P., Salvador, C. R., & Javier, S. G. (2025). Does AI private investment really matter for financial institutions' efficiency? Evidence from a country panel. Finance Research Open, 1, 100009. https://doi.org/10.1016/j.finro.2024.100009

[27] Petter, S., DeLone, W., & McLean, E. (2008). Measuring information systems success: Models, dimensions, measures, and interrelationships. European Journal of Information Systems, 17(3), 236–263. https://doi.org/10.1057/ejis.2008.15

[28] Phi-Hung, N., The-Vu, P., Lan-Anh, T. N., Hong-Anh, T. P., Thu-Hoai, T. N., & Tra-Giang, V. (2024). Assessing cybersecurity risks and prioritising top strategies in Vietnam's finance and banking system using strategic decision-making models based on neutrosophic sets and Z-number. Heliyon, 10, e37893. https://doi.org/10.1016/j.heliyon 2024.e37893

[29] RGP. (2025, July 10). AI in financial services 2025. https://rgp.com/research/ai-in-financial-services-2025/

[30] Sedera, D., & Gable, G. (2010). Knowledge management competence for enterprise system success. Journal of Strategic Information Systems, 19(4), 296-306. https://doi.org/10.1016/j.jsis.2010.10.001

[31] Shulha, O., Yanenkova, I., Kuzub, M., Muda, I., & Nazarenko, V. (2022). Banking information resource cybersecurity system modelling. Journal of Open Innovation: Technology, Market, and

Complexity, 8(2), 80. https://doi.org/10.3390/joitmc8020080

[32] Tam, C., & Oliveira, T. (2016). Understanding the impact of m-banking on individual performance: DeLone & McLean and TTF perspective. Computers in Human Behaviour, 61, 233–244. https://doi.org/10.1016/j.chb.2016.03.016

[33] U.S. Department of the Treasury. (2024, March 27). U.S. Department of the Treasury releases report on managing artificial intelligence-specific cybersecurity risks in the financial services sector. https://home.treasury.gov/news/press-releases/jy2212

[34] Valentin, L. H., & Bruno, D. (2025). Machine learning in banking risk management: Mapping a decade of evolution. International Journal of Information Management Data Insights, 5, 100324. https://doi.org/10.1016/j.jjimei.2024.100324

[35] Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. Management Science, 46(2), 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926

[36] Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425–478. https://doi.org/10.2307/30036540

[37] World Economic Forum. (2024). Global cybersecurity outlook 2024. https://www.weforum.org/reports/global-cybersecurity-outlook-2024