UKR Journal of Economics, Business and Management (UKRJEBM)
Homepage: https://ukrpublisher.com/ukrjebm/
Email: submit.ukrpublisher@gmail.com
Volume 1, Issue 8, 2025
ISSN: 3049-429X (Online)

Strategic Responses in Cybersecurity Management Adopted by Fintechs in Nairobi, Kenya.

Duncan Eric Ogonji [1*], Fred Newa [2]

[1]MSc. Computer Systems, MBA Strategic Management, United States International University Africa.
[2]B.Arch, MBA, International Business, United States International University Africa.

***Corresponding Author**: Duncan Eric Ogonji
DOI: *https://doi.org/10.5281/zenodo.17376604*

Article History
Original Research Article
Received: 09-10-2025
Accepted: 15-10-2025
Published: 17-10-2025

Citation: Duncan Eric Ogonji, Fred Newa. (2025). Strategic Responses in Cybersecurity Management Adopted by Fintechs in Nairobi, Kenya. UKR Journal of Economics, Business and Management (UKRJEBM), Volume 1(issue 8), 01-12.

Abstract

The study adopted a descriptive correlational research design. The target population for the study included 372 professionals in fintechs in Nairobi County. Stratified random sampling was applied by dividing the fintech population in Nairobi County into strata based on job roles. The sample size was computed using the Yamane (1967) formula to arrive at 192 fintech professionals. Primary data collection was based on a structured questionnaire that was scored on a five-point Likert scale. Analysis of data was done via SPSS Version 25.0, and both descriptive and inferential statistics were generated and with output of the analysis expressed as frequencies and percentages and presented in the form of tables and figures.

The study found that regular cybersecurity audits had a mean score of 4.07 (SD = 1.01), the organization of external workshops scored 3.16 (SD = 1.24), and cross-training scored 3.36 (SD = 1.08). The Pearson correlation analysis indicated a strong positive relationship ($r = .576$, $p < .001$) between organizational learning strategies and cybersecurity management. The R^2 value was .332, with a significant ANOVA F-statistic of 71.609. The regression coefficient for organizational learning was .868, suggesting that each unit increase in organizational learning led to an estimated .868 unit increase in cybersecurity management.

The study found that fintechs' incorporation of cybersecurity features into products scored a mean of 3.92 (SD = 0.84), participation in hackathons scored 3.11 (SD = 1.47), and new product development scored 3.25 (SD = 1.32). Pearson correlation analysis indicated a strong positive relationship ($r = .761$, $p < .001$) between continuous innovative strategies and cybersecurity management. The R^2 value was .579, with a significant ANOVA F-statistic of 198.038. The regression coefficient for continuous innovative strategies was .910, suggesting that each unit increase in these strategies led to a .910 unit increase in cybersecurity management.

The study concludes that fintech companies prioritize regular cybersecurity training sessions to ensure a prepared workforce. It further concludes the presence of active investment in innovative cybersecurity solutions, yet limited opportunities fostering employee-driven innovation through hackathons. Moreover, the study concludes that strong internal efforts tend to foster cybersecurity knowledge among staff through training programs. It also concludes there is weak involvement in collaborating with regulatory bodies to stay updated on cybersecurity regulations.

Index Terms *– Fintech, Cybersecurity, Strategy, Financial, Technology.*

1. INTRODUCTION

Cybercrime presents an ever-growing threat, with costs projected to escalate to $10.5 trillion by 2025[1]. In 2024, global cybercrime is set to incur $9.5 trillion in costs, marking a 15 percent rise in global damage expenses over the next two years. The United States leads in data breach costs, averaging $5.09 million in 2023. Security professionals note a 75 percent surge in cyberattacks, with the global average data breach cost hitting $4.45 million in

2023 [2]. [3] report a 50 percent spike in US cyber insurance premiums in 2022, totaling $7.2 billion.

Fintech, the integration of financial services and technology, revolutionizes sectors like lending and payments, yet poses security and privacy risks [4]. [5] found 43% of fintech firms faced data breaches, underscoring evolving cybersecurity challenges. Reported breaches in the financial sector surged from 187 in 2021 to 640 in 2022/23. Brazil, a fintech frontrunner, witnessed heightened cybersecurity investments, exceeding 2019 levels, driven by Moody's US$700 million acquisition of Regulatory DataCorp Inc [6].

Fintech is a pivotal force in Sub-Saharan Africa (SSA), addressing challenges like low financial inclusion, underinvestment, poor infrastructure, and low financial literacy [7]. The fintech sector is growing rapidly in East Africa, particularly in Kenya, and has significantly impacted the underserved population by enabling access to financial services [8].

Cybersecurity challenges include a shortage of professionals, evolving cybercriminal tactics, and threats to critical infrastructure, emphasizing the need for robust cybersecurity measures. Kenya faced a severe loss of $153 million in cybercrime in 2022, projected to increase annually by 14 percent. The country's cybersecurity challenges include escalating cyberattacks targeting diverse vulnerabilities, a scarcity of cybersecurity professionals, and cybercriminals' adoption of advanced technologies like generative AI.

Nairobi city has emerged as a global hub for fintech innovation, driven by its high mobile penetration rates and pioneering services like M-Pesa by Safaricom, which has revolutionized mobile money transfers since 2007 and expanded to other African countries [9]. Fintech activities in Kenya span mobile payments, digital lending, asset and wealth management, insurance, and money remittance operations [10]. They offer a wide range of innovative financial services. Hela Money provides a Remittance account, insurance account, savings account, and virtual cards while Chumz.io offers a platform for saving and investing using gamification and behavioral psychology. KiotaPay provides property management software. Mauzo offers business analytics for MSMEs and SasaPay is a mobile money e-wallet, while BasiGo offers electric alternatives for public buses [11]. However, cybersecurity remains a significant obstacle to Kenya's financial inclusion growth, potentially eroding the country's innovative culture and global fintech market position.

The failure to effectively address cybersecurity can trigger financial losses which result from unauthorized access to customer accounts or payment systems, leading to theft or fraudulent transactions [12]. Cybersecurity breaches can also damage the reputation of fintechs, as customers may lose trust in their ability to protect their sensitive information. Moreover, legal and regulatory consequences may include fines or lawsuits from affected customers [13]. Besides, Operational disruption can lead to downtime and loss of productivity, further affecting the company's ability to serve customers and generate revenue [11].

Studies on the local fintech sector have explored the impact of cybercrime on commercial banks in Kenya. [14] highlighted the vulnerability of electronic banking to cyberattacks, leading to billions of shillings in losses. [15] explored the cybersecurity threats and vulnerabilities faced by Kenyan banks, focusing on weaknesses in soft-ware, hardware, or procedures. [16] examined cyber threats and cybersecurity measures within the Kenyan business landscape, identifying the most prevalent threats and corresponding security measures. [11] studied Ken-ya's fintech policy and regulatory landscape, revealing sector-specific regulations and a "test and learn" approach with regulatory sandboxes

2. LITERATURE REVIEW

The study reviewed empirical studies on influence of organizational learning strategies, continuous innovative strategies, and strategic collaboration on cyber security management in fintech companies.

2.1. Organizational Learning Strategies and Management of Cyber Security among Fintechs

The section reviewed empirical studies on the influence of organizational learning strategies, including knowledge acquisition, skill development, and feedback mechanisms, on cyber security management in fintechs. In addition, the study discusses the management of cyber security among fintechs.

2.1.1. Management of Cybersecurity among Fintechs

Fintech companies are expected to conduct thorough due diligence on vendors, ensure robust cybersecurity measures, and conduct regular audits to comply with contracts, as insider threats pose a significant cybersecurity risk [17]. [18] proposed a machine learning-based framework for cyber threat attribution in the FinTech sector. [19] investigated the growth of FinTech during COVID-19 in the Middle East and North Africa (MENA) region. Their study highlighted privacy issues, cybercrimes, financial disruption, and regulatory non-compliance as major challenges faced by FinTech startups in the region.

In another study, [20] conducted a comparative analysis of cybersecurity in U.S. and Nigerian banking sectors. They highlighted the importance of robust cybersecurity measures in safeguarding financial institutions in the digital

age. The study identified unique challenges and solutions for each country, emphasizing the need for continuous investment in research, collaboration, education, and agile policymaking. [21] performed a systematic literature review on the role of trust and security in Fintech adoption in banking. Their analysis of 26 articles highlighted the importance of trust, security, and other factors in Fintech adoption. The review provided insights into the preferred attributes of Fintech services for enhancing adoption in the banking sector. In addition, findings also suggested that private banks were more flexible in adopting FinTech services compared to public banks, and client attitudes towards FinTech varied across different regions. Locally, [22] studied the effect of the Internet of Things (IoT) and cyber security on FinTech companies in Kenya. Their mixed-method research design surveyed 66 FinTech companies and found that security configuration and system configuration were significant determinants of cyber-attacks among these companies.

2.1.2. Knowledge Acquisition

Knowledge acquisition refers to the process of acquiring, assimilating, and integrating new knowledge and information [23]. Knowledge acquisition is essential for organizations to remain competitive, innovate, and adapt to business changes [24]. It can be achieved through various methods, including research and development (R&D), training and development, external sources like industry reports, and partnerships and collaborations. [25] add that companies can also acquire other companies to access their knowledge, technology, and market presence. [26] opined that information systems and databases are used to access relevant knowledge. Benchmarking helps identify best practices and areas for improvement. Finally, learning from past experiences helps improve future decision-making and actions.

Empirically, [27] discussed the importance of managing cyber risk in the context of enterprise risk, emphasizing the need for executives to connect security technologies to relevant outcomes. The study provided actionable qualitative and quantitative advice on cyber-risk management, offering tools for making the business case and adopting practical strategies.

[28] explored the desired cybersecurity skills and skills acquisition methods in organizations. The study highlighted the importance of key personnel and their competencies in improving cybersecurity resilience. The findings revealed a demand for communication and situational awareness skills, with a specific need for training using Cyber Ranges (CR). The study suggested that systematic cybersecurity training could enhance expertise development and improve performance in complex cybersecurity situations. [29] investigated the impact of cyber security implementation strategy on organizational knowledge management and performance using a case study of Sinapi Aba Savings and Loans in Ghana. The study proposed a conceptual model showing the relationship between knowledge management processes, security compliance, and organizational performance. The results indicated that organizational knowledge management significantly influenced performance, suggesting the importance of integrating cyber security with knowledge management processes.

2.2. Continuous Innovative Strategies and Management of Cyber Security Among Fintechs

The section focuses on the impact of continuous innovative strategies, such as investment in research and development, and process improvement, on cyber security management within the fintech sector.

2.2.1 Investment in research and Development

Investment in R&D is crucial for fintech companies to develop innovative cyber security solutions, including encryption algorithms, advanced threat detection systems, and emerging technologies like AI and blockchain [30]. Fintech companies establish dedicated labs for research and development, collaborate with universities to access cutting-edge research and talent, and organize hackathons to encourage innovation and develop new tools and techniques. These investments help fintech companies maintain a competitive advantage in the market [31].

[32] studied the optimal cyber security investment in a mixed risk management framework, focusing on the role of cyber insurance and expenditure analysis. The study used a mathematical model to explore the effectiveness of integrating insurance and security investments to minimize overall security expenses. However, the findings lacked a detailed examination of various aspects of research and development in cyber security management, which could have provided insights into innovative strategies for addressing cyber risks. [33] discussed the history of cyber security research and focused on cyber risk management, highlighting gaps in research and future directions. The study used a review approach to analyze research on individual steps of the cyber risk management process. However, the findings were limited by the lack of emphasis on the importance of research and development in cyber security management, which could have provided practical solutions for enhancing cyber resilience.

[34] provided an overview of the evolution of cybersecurity research and focused on cyber risk management. The study highlighted gaps in research and emphasized the need for interdisciplinary collaboration to enhance cyber resilience. The two main findings are that cyber risk is difficult to include in the overall enterprise risk management process and that a move toward cyber

resilience is necessary to deal with such a complex risk. However, the study did not extensively discuss the potential impact of research and development in cyber security management on improving cyber risk management practices.

2.2.2 Process Improvement

Process improvement is a crucial aspect of organizational efficiency, quality, and effectiveness. In fintech, it's crucial to enhance cyber security practices by implementing robust incident response procedures, automating security monitoring, and regularly updating policies [35]. Forms in fintech companies include security automation, regular audits, and employee training to reduce human error, identify vulnerabilities, and ensure employees are aware of security best practices. [36] studied cyber situation awareness in the Swedish financial sector, investigating the information elements needed for a common operational picture and exploring key actors' perceptions of cyber-threats. While the sector had a well-developed crisis management concept, there were gaps in systematically collecting and analyzing information about rational adversaries. The study highlighted concerns about cyber-threats to financial infrastructure, IT service availability, data confidentiality, and reputational loss. It suggested integrating cyber personnel into crisis management teams to enhance risk management practices.

[37] conducted a comprehensive analysis of cybersecurity strategies in modern organizations, focusing on the evolution and effectiveness of measures for data protection. The study explored the historical development, current trends, and future directions of cybersecurity strategies, highlighting the shift towards advanced technologies like AI and ML. The findings underscored the importance of human factors, such as continuous education and training, in cybersecurity outcomes. However, the study lacked depth in discussing the specific challenges and strategies for implementing cybersecurity measures, limiting its practical applicability for organizations.

[38] proposed a framework for the future of cybersecurity, aiming to enhance organizational resilience against modern cyber threats. The framework emphasizes the integration of capabilities with resilience, focusing on predicting, mitigating, responding to, and recovering from cyber disasters. The study highlights the importance of organizational leadership, accountability, and innovation in achieving cyber resilience. While the framework provides strategic guidance, it lacks empirical validation and practical implementation guidelines, limiting its immediate applicability for organizations.

2.2.3 New Product Development

New product development is the process of creating innovative solutions for fintech companies to meet evolving customer needs and address cyber security challenges [39]. This includes developing secure mobile payment apps, blockchain-based identity verification systems, and AI-powered fraud detection tools. The fintech companies use agile development methodologies, user-centric design, and compliance integration to ensure products are intuitive, secure, and comply with regulatory requirements related to cyber security [40].

[41] investigated the influence of external factors on supply chain risk management (SCRM) in small and medium-sized enterprises (SMEs) in Turkey. They used fuzzy set qualitative comparative analysis (fsQCA) with data from 137 Turkish SMEs. Results showed different paths for SCRM in young and mature SMEs, with demand risk being crucial for young SMEs and demand risk along with relative performance being essential for mature SMEs. The study provides insights for practitioners to align strategies for SCRM performance based on external factors. [42] examined the relationship between technological, marketing, organizational, and commercialization risk management on new product development (NPD) performance in the automotive industry in Iran. The study suggests that spreading risk management across all aspects of NPD projects can increase total performance and the probability of NPD success, emphasizing the importance of market research and comprehensive risk management in NPD. The research had limitations, including a small sample size and data collected from Iranian automotive producers, which may limit the generalizability of the findings.

[41] explored the multifaceted field of cyber risks, their structure, and composition, focusing on the challenges posed by rapid digital technology evolution. They highlighted the prevalence of cyber risks across various sectors and the vulnerabilities faced by users, organizations, and governments. The importance of robust risk management strategies was emphasized, along with the dynamic nature of cyber threats. The paper reviewed international standards, frameworks, and cyber risk management techniques. It discussed approaches to defining cyber risk categories and analyzed daily attack techniques. The study underscored the need for continuous adaptation of organizational and technical actions to address cyber threats effectively.

3. RESEARCH METHODOLOGY

[43] defines research design as a plan for selecting subjects, research sites, and data collection procedures to answer the research question(s). The study employed a descriptive correlational design. A descriptive correlational design is a type of quantitative research design that focuses on describing and examining the relationships between variables without manipulating them. This non-

manipulative approach allowed for a more natural study of cybersecurity strategies within fintech organizations. The design also facilitated quantitative analysis, providing statistical insights and enhancing the study's rigor and validity.

Population of research is defined as the people whom appeal to the interest of the researchers in generalizing the outcomes of the research [44]. The target population for the study included 93 Chief Information Security Officers (CISOs), 93 Chief Technology Officers (CTOs), 93 Risk Managers, and 93 Compliance Officers in fintechs in Nairobi County. This ensured representation from key roles in cybersecurity management, allowing for a comprehensive analysis of strategic responses. The target population distribution of 372 professional in the field of cybersecurity was shown in Table 3.1.

***Table 3.1**: Target Population Distribution*

Stratum	Population	Percent
Chief Information Security Officers	93	25%
Chief Technology Officers	93	25%
Risk Managers	93	25%
Compliance Officers	93	25%
Total	372	100%

Source: Human Resource Department of Fintech Firms

The study employed a stratified random sampling technique. Stratified random sampling (also known as proportional random sampling and quota random sampling) is a probability sampling technique in which the total population is divided into homogeneous groups (strata) to complete the sampling process. The technique was applied by dividing the fintech population in Nairobi County into strata based on job roles (CISOs, CTOs, Risk Managers, Compliance Officers).

The sample size was computed using [45] formula as follows:

n = N/(1+N(e)2.
n = 372/(1+372(0.05)2.
Given: N=372 e=0.05
n = 192

Therefore, the sample size required became 192 fintech professionals.

***Table 3.2:** Sample Distribution*

Stratum	Population	Percent
Chief Information Security Officers	48	13%
Chief Technology Officers	48	13%
Risk Managers	48	13%
Compliance Officers	48	13%
Total	192	52%

The study used quantitative primary data. Quantitative data collection techniques are based on numerical values and are more amenable to statistical analysis. Questionnaires were employed, which is a method of collecting data in which a selected group of participants are asked to complete a written set of questions to find out what they do, think, or feel [46]. The questionnaire was structured and included the following sections: section one targeted the background information of the respondents, section two focused on the influence of organizational learning strategies in the management of cybersecurity, section three covered the influence of continuous innovative strategies in the management of cybersecurity, and section four examined the influence of strategic collaboration in the management of cybersecurity among fintechs. The questionnaire included Likert scale questions ranging from 1 (strongly agree or never) to 5 (strongly disagree or very often), which were used to measure the factor variables affecting the strategic responses adopted by fintechs in the management of cybersecurity. These questions required the respondents to indicate to what extent they agreed with the statements cited in each of the factor variables.

A pilot study on 20 fintech professionals was conducted to analyze questions and assess their validity. This was crucial for identifying well-framed and ambiguous questions. A pre-test was used to evaluate respondents' interest. Furthermore, pilot studies are essential for analyzing response time and validity. The Cronbach Alpha test was employed to examine the reliability of the questionnaire, and according to [45] Barbera, Naibert, Komperda, and Pentecost (2021), the coefficient threshold set for reliable instruments was ≥0.7. The reliability test analyses confirmed that all the Cronbach's alpha coefficients were above 0.7 hence reliability of the results. Afterward, the researcher administered the refined questionnaires to the respondents to ensure a timely response via Survey Monkey.

***Table 3.3**: Reliability Results*

Variable	No. of Items	Cronbach's Coefficient	Decision
Organizational Learning Strategies	12	0.784	Reliable
Countinous Innovation Strategies	12	0.851	Reliable
Strategic Collaboration Strategies	12	0.726	Reliable
Management of Cyber Security	12	0.803	Reliable
Average	12	0.791	Reliable

Descriptive statistics were used to analyze the collected data. The descriptive statistics included the use of the mean, frequency, and percentages. According to [47], the procedure of transforming raw data into charts, tables with percentages, and distribution frequencies is referred to as

descriptive statistics. Moreover, inferential statistics were also utilized in this research to quantify the relationship between the dependent and independent variables through the application of simple linear regression and Pearson coefficient correlation analysis [48]. The Pearson correlation coefficient analysis was key in providing an assessment of the level of association present between factors affecting performance of insurance firms. The simple linear regression analysis was fundamental in providing the weighting of the individual factors. The analysis of data was displayed through the use of tables and figures.

$$Y = \beta 0 + \beta 1X1 + \beta 2X2 + \beta 3X3 + \varepsilon$$

Where;
Y= Management of Cybersecurity
β0= constant
β1……β3 =coefficients
X1= Organizational Learning Strategies
X2 = Continuous Innovative Strategies
X3= Strategic Collaboration
ε = error term

4. RESULTS

The results and findings of the study including back-ground information, response rate and demographic de-tails of participants is represented using descriptive statistics, Pearson correlation and regression analysis.

The study attained a response rate of 76% as revealed in figure 4.1. The rate was considered adequate to allow for data analysis.

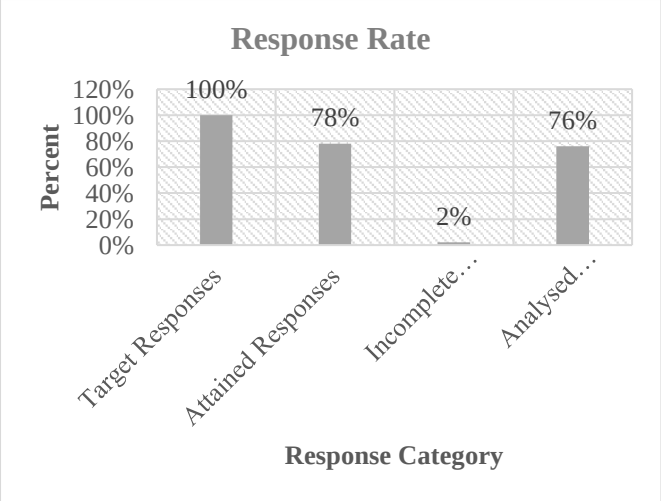

Figure 4.1: Response Rate

According to Figure 4.2, the study found that Chief Technology Officers (CTOs) played the most significant role in managing cybersecurity in Nairobi County fintechs, with 39% of respondents identifying them as key figures. The Chief Information Security Officers (CISOs) were also crucial, representing 26% of the roles involved. On the other hand, Compliance Officers accounted for 19%, highlighting their importance in ensuring adherence to cybersecurity regulations. Moreover, Business System Analysts and Business Development Managers contributed 11% and 5%, respectively.

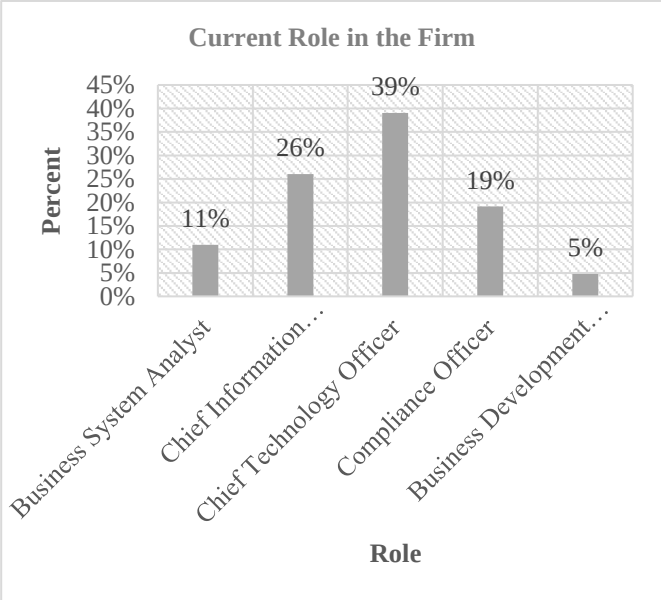

Figure 4.2: Current Role in the Firm

According to Figure 4.3, the study revealed that Bachelor's Degree holders constituted the majority of respondents involved in managing cybersecurity in Nairobi County fintechs, accounting for 53%. This level of education was followed closely by those with a Master's Degree, comprising 42% of the respondents. Diploma holders represented a smaller proportion at 3%, while individuals with a Doctoral Degree were the least represented at 1%. With these results, respondents were literate hence capable of reading, interpreting and answering strategic questions related to cyber security management.

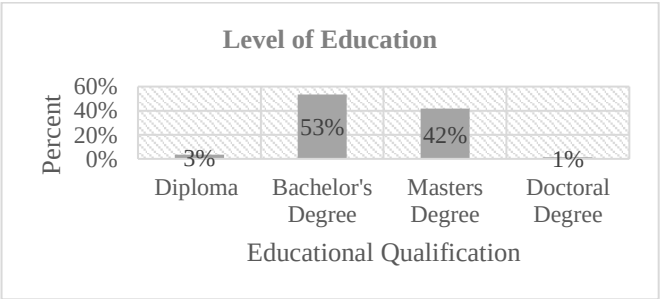

Figure 4.3: Level of Education

According to Figure 4.4, the study found that professionals with 6-9 years of experience constituted the largest group involved in managing cybersecurity in Nairobi County fintechs, accounting for 43% of respondents. Those with 10 years and above of experience followed at 26%, indicating a substantial portion of seasoned professionals in the field. Respondents with 3-5 years of experience represented 18%, while those with less than 3 years accounted for 12%. These

findings emphasize the importance of mid-career and experienced professionals in shaping strategic responses to cybersecurity challenges within the fintech sector in Nairobi County.

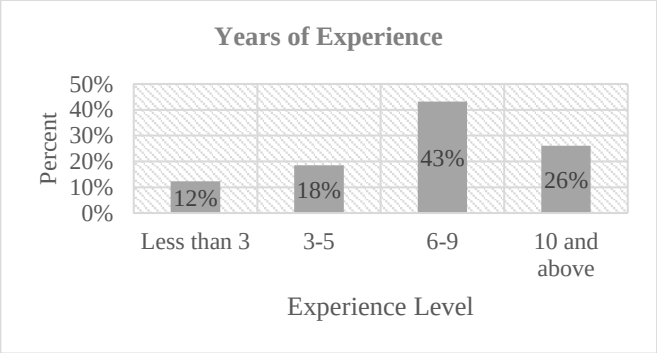

Figure 4.4: Years of Experience

According to Figure 4.5, the study revealed that fintechs in Nairobi County with workforce sizes ranging from 101-500 employees were the most prevalent, comprising 35% of the respondents. Companies with more than 500 employees followed closely at 28%, indicating a substantial presence of larger organizations in the sample. Fintechs with 50-100 employees accounted for 25%, while those with less than 50 employees represented 12% of the respondents. The study outlined the diverse company sizes and organizational capacities in the fintech sector in Nairobi County.

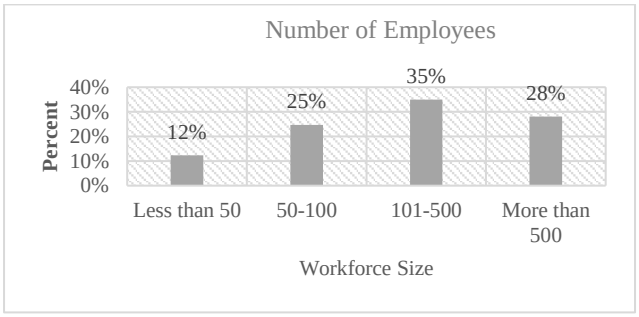

Figure 4.5: Number of Employees

According to Table 4.1, 44.5% of respondents strongly agreed that their fintech reduced the frequency of successful DoS attacks. This indicates effective management practices in mitigating such cyber threats. Moreover, 47.3% agreed that their fintech reduced the occurrence of malware infections, showcasing robust cybersecurity measures in place. Furthermore, 40.4% strongly agreed that their fintech improved its response time to mitigate DoS attacks, suggesting enhanced readiness in handling such incidents. In comparison, 41.1% agreed that their fintech minimized the impact of phishing attacks, indicating effective protection of employees and customers against these threats.

Additionally, 39.7% agreed that their fintech reduced the number of data breaches involving customer information, reinforcing successful data protection strategies with 28.1% strongly agreed that their fintech improved its ability to detect and respond to data breaches promptly, indicating heightened cybersecurity vigilance; and 34.2% strongly agreed that their fintech minimized the impact of data breaches on its reputation and customer trust, showing efforts to maintain customer confidence amidst security challenges.

The highest standard deviation was noted in the statement about maintaining full compliance with relevant cybersecurity regulations and standards (1.01), explained by differing levels of regulatory requirements and compliance capabilities across different fintech firms. The lowest standard deviation was found in the statement concerning the reduction of successful DoS attacks (0.72), indicating a more consistent performance across firms in this area.

Table 4.1: *Rating for Management of Cyber Security Among Fintechs*

Statement	SD(%)	D(%)	N(%)	A(%)	SA(%)	Mean	Std Dev
Reduced frequency of successful DoS attacks	0.0	0.0	15.1	40.4	44.5	4.29	0.72
Reduced occurrence of malware infections	0.0	4.8	11.0	47.3	37.0	4.16	0.81
Improved response time to mitigate DoS attacks	2.7	0.0	13.0	43.8	40.4	4.19	0.87
Minimized impact of phishing attacks	0.0	4.8	17.1	41.1	37.0	4.10	0.85
Reduced number of data breaches involving customer information	0.0	2.7	29.5	39.7	28.1	3.33	0.83
Improved ability to detect and respond to data breaches in a timely manner	0.0	2.7	29.5	39.7	28.1	3.42	0.93
Minimized impact of data breaches on reputation and customer trust	0.0	2.7	31.5	31.5	34.2	3.57	0.88
Mitigated risk of insider threats through improved monitoring and access control	2.7	2.7	21.9	44.5	28.1	3.99	0.98
Maintained full compliance with relevant cybersecurity regulations and standards	5.5	2.1	6.8	47.9	37.7	4.10	1.01
Improved regulatory audit scores related to cybersecurity	2.7	0.0	15.1	45.2	37.0	4.14	0.87
Reduced regulatory fines or penalties related to cybersecurity non-compliance	2.7	2.1	4.1	41.8	49.3	4.33	0.87
Enhanced cybersecurity policies and procedures to meet or exceed regulatory requirements	0.0	2.7	17.8	39.0	40.4	4.17	0.82

KEY: SD (Strongly Disagree) D (Disagree) N (Neutral) A (Agree) SA (Strongly Agree), Std Dev - Standard Deviation.

According to Table 4.2, fintech companies demonstrated various levels of organizational learning strategies related to cybersecurity management. For instance, 37% strongly agreed that their fintech conducted regular cybersecurity training sessions for employees, indicating a robust focus on employee knowledge enhancement. Conversely, 32.2% were neutral, suggesting inconsistencies in training implementation. Similarly, 49.3% agreed that their fintech had a system for employees to provide feedback on cybersecurity policies, emphasizing the value placed on employee input. However, 27.4% were neutral about knowledge-sharing platforms, highlighting a potential area for improvement in disseminating best practices.

Furthermore, 41.1% strongly agreed that regular cybersecurity audits were conducted and used to improve practices, reflecting a commitment to continuous improvement. Meanwhile, 33.6% were neutral about encouraging employees to pursue cybersecurity certifications, indicating varied support for formal skill development. Additionally, 53.4% agreed that cybersecurity awareness campaigns were conducted, showing proactive measures against emerging threats. Yet, 33.6% were neutral regarding organizing external workshops, possibly due to budget or logistical constraints.

Moreover, 46.6% agreed that open communication channels for reporting cybersecurity incidents were encouraged, signifying the importance of incident reporting. However, 33.6% were neutral on cross-training between departments, suggesting an area for broader understanding improvement. In terms of mentorship, 32.2% agreed that programs were offered to enhance skills, while 24.7% were neutral, indicating room for better support. Lastly, 31.5% strongly agreed that a culture of continuous improvement based on feedback was established, underlining the industry's dedication to evolving cybersecurity practices, although 25.3% were neutral, indicating varied experiences across firms.

Regarding the mean ratings, regular cybersecurity audits and their utilization for practice improvement scored 4.07 (Std. Deviation = 1.01). The high score indicates robust practices in auditing and leveraging findings for continuous cybersecurity enhancement, demonstrating proactive management of cybersecurity risks. Also, the organization of external cybersecurity workshops or seminars received a mean score of 3.16 (Std. Deviation = 1.24). This lower score indicates limited external engagement for skill development, possibly influenced by resource constraints or a focus on internal training methods.

Table 4.2: *Descriptive Statistics for Organizational Learning Strategies in Fintechs*

Statement	SD (%)	D (%)	N (%)	A (%)	SA (%)	Mean	StDev
Regular cybersecurity training sessions for employees	2.7	0.0	32.2	28.1	37	3.97	0.97
Knowledge sharing platforms for cybersecurity best practices	7.5	9.6	27.4	30.1	25.3	3.56	1.19
Encouraging cybersecurity certifications or courses	7.5	6.8	33.6	35.6	16.4	3.47	1.08
Cybersecurity awareness campaigns for emerging threats	4.8	0.0	14.4	53.4	27.4	3.99	0.92
Opportunities for cybersecurity-related projects or simulations	7.5	9.6	24.7	34.9	23.3	3.57	1.17
Mentorship programs to enhance cybersecurity skills	10.3	13.7	24.7	32.2	19.2	3.36	1.23
Cross-training between departments for broader cybersecurity understanding	7.5	11.6	30.1	38.4	12.3	3.36	1.08
External cybersecurity workshops or seminars	13	13.7	33.6	23.3	16.4	3.16	1.24
System for feedback on cybersecurity policies	9.6	4.8	26	49.3	10.3	3.46	1.06
Regular cybersecurity audits and improvements based on results	2.7	4.8	16.4	34.9	41.1	4.07	1.01
Open communication channels for reporting cybersecurity incidents	5.5	0.0	25.3	46.6	22.6	3.81	0.97
Culture of continuous improvement in cybersecurity	2.7	4.8	25.3	35.6	31.5	3.88	1.00

Table 4.3 presented findings from Pearson correlation analysis between Organizational Learning Strategies and Management of Cyber Security among fintechs. The correlation coefficient (r) of .576** indicates a strong positive relationship between the two variables. The p-value (.000) indicates this correlation is highly significant at the 0.01 level (2-tailed), suggesting that as organizational learning strategies improve, so does the management of cyber security within fintechs.

Table 4.3: Pearson Correlation Analysis between Organizational Learning Strategies and Management of Cyber Security Among Fintechs

		Organizational Learning	Management of_Cyber_Security
Organizational Learning	Pearson Correlation	1	.576**
	Sig. (2-tailed)		.000
	Sum of Squares and Cross-products	59.786	51.885
	Covariance	.412	.358
	N	146	146
Management of Cybersecurity	Pearson Correlation	.576**	1
	Sig. (2-tailed)	.000	
	Sum of Squares and Cross-products	51.885	135.579
	Covariance	.358	.935
	N	146	146

**. Correlation is significant at the 0.01 level (2-tailed).

5. DISCUSSION

The general objective of the study was to investigate the strategic responses adopted by fintechs in the management of cybersecurity in Nairobi County. The study aimed to address the following specific objectives: Firstly, to investigate the influence of organizational learning strategies in the management of cybersecurity among fintechs in Nairobi County; secondly, to establish the influence of continuous innovative strategies in the management of cybersecurity among fintechs in Nairobi County; and finally, to examine the influence of strategic collaboration in the management of cybersecurity among fintechs in Nairobi County.

The study adopted a descriptive correlational research design. The target population for the study included 372 professionals: 93 Chief Information Security Officers (CISOs), 93 Chief Technology Officers (CTOs), 93 Risk Managers, and 93 Compliance Officers in fintechs in Nairobi County. Stratified random sampling was applied by dividing the fintech population in Nairobi County into strata based on job roles. The sample size was computed using [45] formula to arrive at 192 fintech professionals. Primary data collection was based on a structured questionnaire scored on a Five-point Likert scale.

The study found that fintech companies demonstrated

various levels of organizational learning strategies related to cybersecurity management. In support, [17] emphasized the importance of policies, risk management strategies, and regular employee training in managing cybersecurity. Similarly, [49] mentioned the benefits of such management practices in enhancing business continuity and customer trust. However, these results contrast with [50], who pointed out significant challenges including privacy issues and regulatory non-compliance in the MENA region's fintech startups, indicating regional differences in the implementation of cybersecurity strategies.

Likewise, the study revealed that conducting regular cybersecurity training sessions was a common practice among fintechs. This result aligns with the observation by [51], who underscored the need for continuous employee education to prevent and mitigate cyberattacks. [52] also emphasized the importance of training in their examination of cybersecurity risk assessment in banking. Conversely, [53] found that many Nigerian MSEs lacked awareness and channels for reporting cyber incidents, suggesting that training alone may not suffice without proper reporting mechanisms.

It was further established that knowledge sharing platforms were moderately utilized by fintech companies to disseminate cybersecurity best practices. This approach is in agreement with the recommendations of [54], who advocated for the integration of various organizational learning strategies to enhance performance. [55] also supported this by linking organizational learning strategies with resilience in dynamic environments. However, the study by [20] noted unique challenges in the U.S. and Nigerian banking sectors, where knowledge sharing was hindered by differences in regulatory frameworks and technological infrastructures.

Nonetheless, the encouragement for employees to pursue cybersecurity certifications or courses reflected moderate support for skill enhancement through formal education. The results resonate with [56], who emphasized the need for continuous education and training to cope with evolving cybersecurity threats. [57] also opined the im-portance of training in their proposed learning loop framework for cybersecurity in higher education. How-ever, the study by [17] in Egypt identified regulatory challenges that could limit the effectiveness of formal education initiatives.

The study found robust efforts in conducting cybersecurity awareness campaigns to educate employees about emerging threats. This aligns with the work of [58], who both stressed the importance of awareness programs in preventing cyber incidents. [59] also noted the effectiveness of simulation-based training in enhancing cybersecurity skills. However, these efforts contrast with the findings of [60], who reported significant cyber-attacks in Kenyan fintechs due to inadequate security configurations, indicating a gap between awareness and practical implementation.

Concerning continuous innovation, fintech companies demonstrated a moderate commitment to researching emerging cybersecurity threats and trends. [61] emphasized the importance of continuous innovation in cyber-security to address evolving threats, suggesting that companies have significant potential for collaborative innovation. This result resonates with [62], who emphasized the need for firms to understand the determinants of innovation persistence. Similarly, [63] outlined the necessity for continuous adaptation to cyber threats, suggesting a proactive approach. In contrast, [64] found that regulatory interventions could play a significant role in encouraging firms to enhance their cybersecurity investments, pointing to external factors rather than internal employee initiatives.

The result reveals that fintechs to leverage technology for efficiency gains through automation tools for cyber-security tasks. This result resonates with [65], who underscored the importance of advanced technological solutions in maintaining a competitive edge. [34] also emphasized the evolution of cybersecurity research, emphasizing technology's role. However, [66] found that integrating cyber personnel into risk management teams is crucial, suggesting that fintechs should balance technological investments with human resource development.

6. CONCLUSION

The study suggests enhancing cybersecurity training sessions by integrating practical simulations to bolster employee preparedness. It also recommends expanding knowledge sharing platforms to ensure consistent adoption of cybersecurity best practices across all departments. Furthermore, it calls for incentivizing cybersecurity certifications and courses to boost skill development. Implementing structured mentorship programs and fostering interdisciplinary training can deepen organization-al cybersecurity resilience.

The study calls for further research in investigating strategies for cybersecurity by expanding the scope to include other industry stakeholders such as the Ministry of ICT, to foster comprehensive regulatory and exploring mechanisms to enhance employee-driven innovation through hackathons and similar initiatives. Further research is also needed to optimize the integration of cybersecurity into overall business strategies to ensure alignment and effectiveness.

APPENDIX

Not applicable

REFERENCES

1. Crisanto, J. C., Pelegrini, J. U., & Prenio, J. (2023). Banks' cyber security – a second generation of regulatory approaches. *FSI Insights on Policy Implementation*, No. 50, Financial Stability Institute, Bank of International Settlements.
2. Hassan, A. O., Ewuga, S. K., Abdul, A. A., & Abrahams, T. O. (2024). Cybersecurity in banking: A global perspective with a focus on Nigerian practices. *Computer Science & IT Research Journal,* 5(1), 41-59. DOI: 10.51594/csitrj.v5i1.701
3. Javaheri, D., Fahmideh, M., Chizari, H., & Lalbakhsh, P. (2021). Cybersecurity Threats in FinTech: A Systematic Review. *Expert Systems with Applications*, 6(6), 1081-1088
4. Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. *Authorea Preprints,* 1(1), 1-12.
5. Kshetri, N. (2020). China's Emergence as the Global Fintech Capital and Implications for Southeast Asia. *Asia Policy*, *15*(1), 61–82. https://www.jstor.org/stable/26891388
6. Trinks, M. D., Albuquerque, R. d. O., Nunes, R. R., & Mota, G. A. (2022). Strategic Assessment of Cyber Security Contenders to the Brazilian Agribusiness in the Beef Sector. *Information,* 13(9), 431-444. https://doi.org/10.3390/info13090431
7. Oyeniyi, A. (2021, November 5). MTN and Airtel get "approval in principle" to launch mobile money services in Nigeria. *Tech Cabal*. https://techcabal.com/2021/11/05/mtn_
8. Misati, R., Kamau, A., Kipyegon, L., & Wandaka, L. (2020). Is the Evolution of Fintech Complementary to Bank Performance in Kenya? *KBA Centre for Research on Financial Markets and Policy*® Working Paper Series, WPS/08/20.
9. Chitavi, M., Cohen, L., & Hagist, S. C. N. (2021, February 18). Kenya Is Becoming a Global Hub of FinTech Innovation. Harvard Business Review, 5(2), 18-27
10. Muthaura, T., Muguna, B. K., & Wandiri, L. (2021). Influence of financial technology on financial performance of commercial banks in Kenya. African Development Finance Journal, 5(2), 45-64.
11. Musamali, R., Jugurnath, B., & Maalu, J. (2023). Fintech in Kenya: A policy and regulatory perspective. *Journal of Smart Economic Growth,* 8(1), 21-53.
12. Mwencha, P. M., Hussein, A., & Githaiga, G. (2019). *Towards an inclusive and sustainable fintech ecosystem in Kenya: Current outlook, challenges, and policy options for the sector. MediaForce Communications.* Kenya ICT Action Network
13. Netshakhuma, N. S. (2023). Cybersecurity Management in South African Universities. *Issues, Challenges, and Solutions in the Business World*, 3(2), 722-741
14. Njeru, P. W., & Gaitho, V. (2019). Investigating the extent to which cybercrime influences performance of commercial banks in Kenya. *International Journal of Economics, Commerce and Management,* 7(8), 489-514.
15. Wakoli, L. W., Ogara, S., & Liyala, S. (2020). An understanding of the cyber security threats and vulnerabilities landscape: A case of banks in Kenya. *International Journal of Disclosure and Governance,* 15(4), 258-263.
16. Ndeda, L. A., & Odoyo, C. O. (2019). Cyber threats and cyber security in the Kenyan business context. *GSJ: Global Scientific Journal*, 7(9), 576-582.
17. Abdelbaset, A. S. (2021). Obstacles of FinTech in Egyptian Bank Sector under Social Distancing. *Scientific Journal for Financial and Commercial Studies and Researche*, 2 (1), 425-454.
18. Noor, U., Anwar, Z., Amjad, T., & Choo, K.-K. R. (2019). A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. *Future Generation Computer Systems*, 96(18), 227-242.
19. Naz, F., Karim, S., & Houcine, A., (2024). Fintech Growth during COVID-19 in MENA Region: Current Challenges and Future prospects. *Electron Commer Res,* 24(2), 371–392.
20. Opoku-Ahene, A. R., & Zwilling, M. (2022). The Influence of Cyber Security Implementation Strategy on Organizational Knowledge Management and Performance – A Case Study of Sinapi Aba Savings and Loans in Ghana. *Social and Business Studies,* 9(4), 119-123
21. Jafri, J. A., Mohd Amin, S. I., Rahman, A. A., & Nor, S. M. (2024). A systematic literature review of the role of trust and security on Fintech adoption in banking. *Heliyon,* 10(1), 22980-22997.
22. Karanja, M. W., & Purity, G. (2024). Internet of Things and Cyber Attacks Among Fintech Companies in Kenya. *Int Journal of Social Sciences Management and Entrepreneurship*, 8(1), 970-983.

23. Dávila, G. A., Cuenca-Jiménez, M. T., & Durst, S. (2023). Knowledge Absorptive Capacity in FinTechs: Evidence from Latin America. *European Conference on Knowledge Management, 24*(1), 293-301. DOI:10.34190/eckm.24.1.1334

24. Al Dmour, R., Dmour, A., Rababeh, N., & Al Dmour, H. (2021). The influence of knowledge management processes on FinTech innovation: Lebanon evidence. *International Journal of Knowledge and Learning, 14*(1), 63-77.

25. Bakri, A. A., WP, D. A., Khaddafi, M., Kusnadi, I. H., & Boari, Y. (2023). The Impact Of Financial Technology On Transactional Knowledge Acquisition Among Generation Z. *Jurnal Scientia*, *12*(03), 3972-3978.

26. Jackson, D., Dunbar, K., Sarkis, J., & Sarnie, R. (2023). Advancing Fintech through a transdisciplinary approach. *iScience, 26*(9), 107694-107709. DOI:10.1016/j.isci.2023.107694

27. Evans, A. (2019). *Managing Cyber Risk* (1st ed.). Routledge.

28. Aaltola, K., Ruoslahti, H., & Heinonen, J. (2022). Desired cybersecurity skills and skills acquisition methods in organizations. *European Conference on Cyber Warfare and Security*, 21(1), 1-9.

29. Rao, P. B. (2024). A study on cyber security issues affecting online banking and transactions. *International Journal of Advanced Research and Innovative Ideas in Education,* 9(6), 635-645.

30. Stulz, R. M. (2019). FinTech, BigTech, and the future of banks. *Journal of Applied Corporate Finance*, 31(4), 86-97.

31. Liu, Q., Chan, K. C., & Chimhundu, R. (2024). Fintech research: systematic mapping, classification, and future directions. *Financial Innovation, 10*(1), 129-144.

32. Mazzoccoli, A. (2023). Optimal Cyber Security Investment in a Mixed Risk Management Framework: Examining the Role of Cyber Insurance and Expenditure Analysis. *Risks, 11*(9), 154-167. https://doi.org/10.3390/risks11090154

33. Mcshane, M., Eling, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review, 24*(6), 98-116.

34. Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review, 24*(1), 93-125. https://doi.org/10.1111/rmir.12169

35. Chahal, S. (2023). Navigating Financial Evolution: Business Process Optimization and Digital Transformation in the Finance Sector. *International Journal of Finance, 8*(5), 67-81.

36. Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. Computers & Security, 105(19), 102239-102251.

37. Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., & Adegbite, A. O. (2024). A review of cybersecurity strategies in modern organizations: Examining the evolution and effectiveness of cybersecurity measures for data protection. *Computer Science & IT Research Journal, 5*(1), 1-25.

38. Safitra, M.F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability, 15(6)*, 13369-13379.

39. Harsono, I., & Suprapti, I. A. P. (2024). The Role of Fintech in Transforming Traditional Financial Services [Peran Fintech dalam Transformasi Layanan Keuangan Tradisional]. *Accounting Studies and Tax Journal (COUNT), 1*(1), 81-91.

40. Saksonova, S., & Kuzmina-Merlino, I. (2019). Fintech as Financial Innovation - The Possibilities and Problems of Implementation. *European Research Studies Journal, 20*(3), 961-973. DOI:10.35808/ersj/757

41. Foli, S., Durst, S., Davies, L., & Temel, S. (2022). Supply chain risk management in young and mature SMEs. *Journal of Risk and Financial Management, 15(7)*, 328.

42. Salavati, M., Tuyserkani, M., Mousavi, S. A., & Falahi, N. (2016). Improving new product development performance by risk management. *Journal of Business and Industrial Marketing, 31*(3), 418-425. https://doi.org/10.1108/JBIM-04-2013-0090

43. Mahat, D. (2024). Quantitative Research Design and Sample Trends: A Systematic Examination of Emerging Paradigms and Best Practices. *Cognizance Journal of Multidisciplinary Studies,* 4(2), 20-27.

44. Willie, M. M. (2022). Differentiating Between Population and Target Population in Research Studies. *International Journal of Medical Science and Clinical Research Studies,* 2(6), 521-523. https://doi.org/10.47191/ijmscrs/v2-i6-14

45. Yaacob, M. N., Syed Idrus, S. Z., & Idris, M. (2023). Managing cybersecurity risks in emerging technologies. *International Journal of Business and*

Technopreneurship, 13(3), 253-270.

46. Ranganathan, P., Caduff, C., & Frampton, C. M. A. (2024). Designing and validating a research questionnaire - Part 2. *Perspectives in Clinical Research,* 15(1), 42-45.

47. Schindler, P. J. (2022). *Business Research Methods* (14th ed.). McGraw-Hill.

48. Okello, G. (2022). *Simplified Business Statistics Using SPSS* (1st ed.). Chapman and Hall/CRC. https://doi.org/10.1201/9781003292654

49. Patterson, C.M., Nurse, J.R.C., & Franqueira, V.N.L. (2024). "I don't think we're there yet": The practices and challenges of organisational learning from cyber security incidents. Computers & Security, 139(15), 103699-103707.

50. Naz, F., Karim, S., & Houcine, A., (2024). Fintech Growth during COVID-19 in MENA Region: Current Challenges and Future prospects. *Electron Commer Res,* 24(2), 371–392. DOI:10.1007/s10660-022-09583-3

51. Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees' information security awareness in private and public organizations: A systematic literature review. *Computers & Security*, 106(17), 102267-102277

52. Elliehausen, G., & Hannon, S. (2023). Fintech and Banks: Strategic Partnerships that Circumvent State Usury Laws. *FEDS Working Paper No. 2023-56.* Available at SSRN:

53. Ikuero, F. E., & Zeng, W. (2022). Improving Cybersecurity Incidents Reporting in Nigeria: Micro and Small Enterprises Perspectives. *Nigerian Journal of Technology*, 41(3), 512-520.

54. Bonime-Blanc, A., & Cottini, A. (2019). Managing Cyber Risk: A Strategic Imperative for Organizations. *Research Journal of Business & Management.* 3(3), 98-108

55. Dubrovski, D. (2020). Characteristics of Strategic Partnerships between Differently Successful Companies. *Journal of Financial Risk Management,* 9(3), 82-98.

56. Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2019). How integration of security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, 71(8), 939-953.

57. Mishra, S. (2023). Exploring the Impact of AI-Based Cyber Security Financial Sector Management. *Applied Sciences*, 13(10), 5875-5888. DOI:10.3390/app13105875

58. Kabanov, I., & Madnick, S. (2021). Applying the Lessons from the Equifax Cybersecurity Incident to Build a Better Defense. MI S Quarterly Executive, 20(2), 109-125.

59. Chowdhury, N., & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review,* 40(9), 1003-1023.

60. Karanja, M. W., & Purity, G. (2024). Internet of Things and Cyber Attacks Among Fintech Companies in Kenya. *Int Journal of Social Sciences Management and Entrepreneurship*, 8(1), 970-983.

61. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 7(8), 8176-8186. DOI: 10.1016/j.egyr.2021.08.126

62. Callen-Naviglia, J., & James, J. (2018). Fintech, Regtech and The Importance of Cybersecurity. *Issues in Information Systems*, 19(3), 220-225.

63. Ohrimenco, S., & Cherny, V. A. (2024). Cybersecurity risk. Economic Security in the Context of Systemic Transformations. Baltic Journal of Economic Studies 9(5):87-93

64. Ahnert, T., Brolley, M., Cimon, D. A., & Riordan, R. (2024). Cyber Risk and Security Investment. *Review of Accounting Studies* , 23(9), 1177 - 1206

65. Stulz, R. M. (2019). FinTech, BigTech, and the future of banks. *Journal of Applied Corporate Finance*, 31(4), 86-97.

66. Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. Computers & Security, 105(19), 102239-102251.