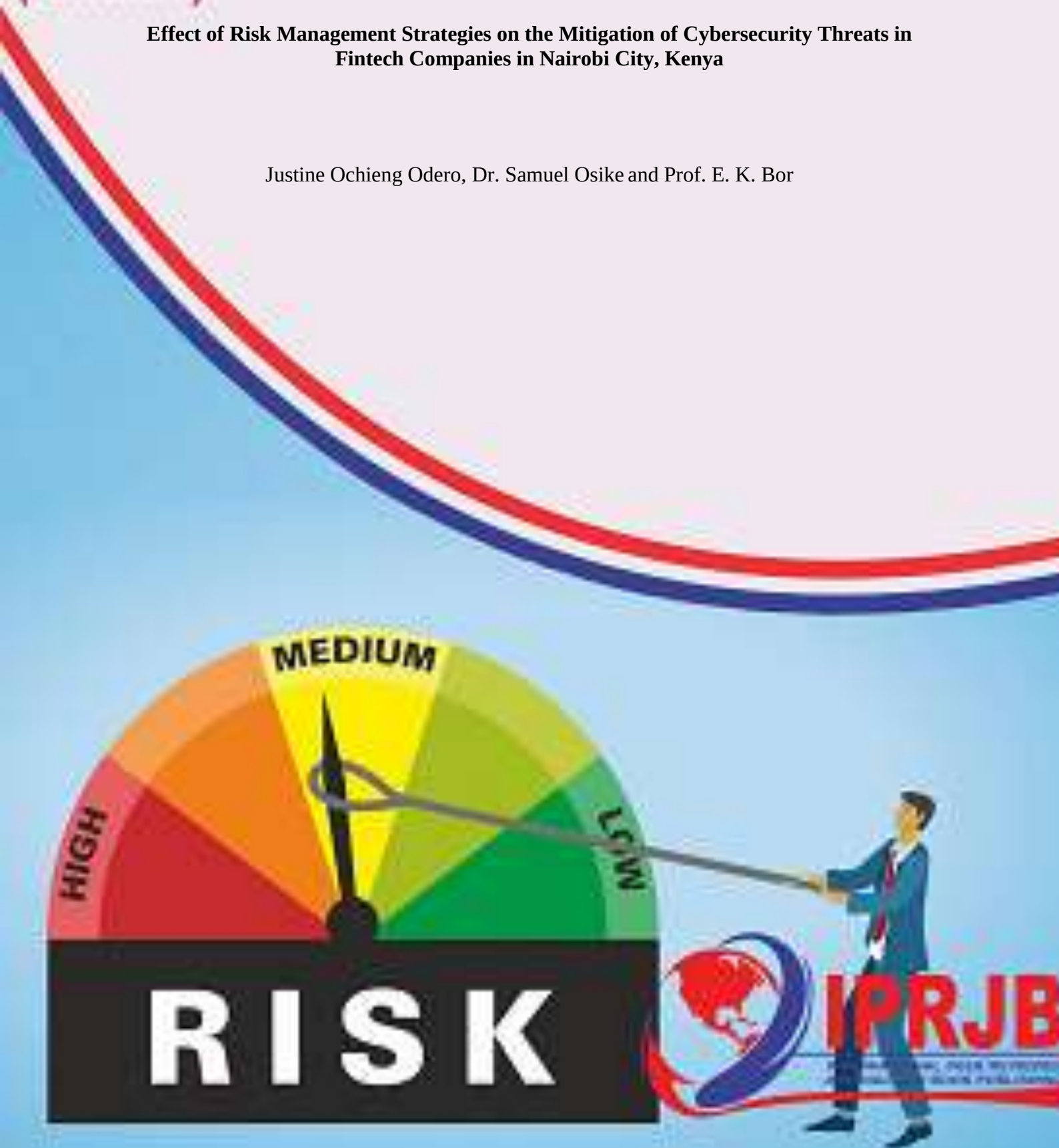


International Journal of Modern Risk Management (IJMRM)

**Effect of Risk Management Strategies on the Mitigation of Cybersecurity Threats in
Fintech Companies in Nairobi City, Kenya**

Justine Ochieng Odero, Dr. Samuel Osike and Prof. E. K. Bor



Effect of Risk Management Strategies on the Mitigation of Cybersecurity Threats in Fintech Companies in Nairobi City, Kenya



Justine Ochieng Odera^{1*}

Postgraduate Student, Department of Peace, Security and Social Studies, Egerton University, Kenya



Dr. Samuel Osike²

Lecturer, Department of Peace, Security and Social Studies, Egerton University, Kenya



Prof. E. K. Bor³

Lecturer, Department of Peace, Security and Social Studies, Egerton University, Kenya

Article History

Received 13th August 2026

Received in Revised Form 19th September 2026

Accepted 16th October 2026



How to cite in APA format:

Odera, J., Osike, S., & Bor, E. (2026). Effect of Risk Management Strategies on the Mitigation of Cybersecurity Threats in Fintech Companies in Nairobi City, Kenya. *International Journal of Modern Risk Management*, 4(1), 15–32. <https://doi.org/10.47604/ijmrm.4014>

Abstract

Purpose: The purpose of this study was to examine the effect of risk management strategies on the mitigation of cybersecurity threats in fintech companies in Nairobi City, Kenya. Specifically, the study identified the cybersecurity threats faced by fintech companies, assessed the types and levels of risk management strategies they employ, and determined the effect of these strategies on threat mitigation.

Methodology: The study adopted a correlational research design anchored on Deterrence Theory and the Resource-Based View. The target population comprised 306 cybersecurity, risk, information technology and compliance professionals drawn from 98 fintech companies in Nairobi City. A sample of 173 respondents was selected through stratified random sampling and 12 key informants were purposively selected. Data were collected using structured questionnaires and key informant interviews, and 145 usable questionnaires were returned (83.8%). Quantitative data were analysed using descriptive statistics, Pearson correlation and multiple regression, while qualitative data were analysed thematically.

Findings: Malware infections were the most prevalent threat ($M = 4.57$, $SD = 0.524$), followed by phishing ($M = 3.46$) and Distributed Denial of Service (DDoS) attacks ($M = 3.41$), although the consequences of DDoS attacks were rated as severe ($M = 3.91$). Regular vulnerability assessments ($M = 3.83$) and threat intelligence gathering ($M = 3.79$) were the most widely implemented practices, while technical controls recorded the lowest level of implementation ($M = 3.52$). Risk management practices were strongly correlated with mitigation ($r = .705$, $p < .01$) and explained 49.8% of the variance in mitigation outcomes ($R^2 = .498$, $F = 141.604$, $p < .01$), rising to 55.6% when threat exposure was added ($R^2 = .556$, $F = 89.050$, $p < .01$). Improved perception of security posture ($M = 4.04$) was rated higher than reduction of the financial impact of attacks ($M = 3.31$), revealing a perception–protection gap.

Unique Contribution to Theory, Practice and Policy: Fintech companies should enforce multi-factor authentication, move from annual to continuous vulnerability scanning, institute role-based awareness training with phishing simulations, and appoint dedicated cybersecurity personnel in proportion to their risk profile. Regulators should harmonise Kenya's fragmented cybersecurity rules into proportionate minimum standards for all categories of fintech, mandate independent security audits for high-volume firms, and operationalise sector-wide threat intelligence sharing. Theoretically, the study shows that deterrence in fintech cybersecurity works mainly through denial rather than punishment, and that resource-based advantage lies in dynamic cybersecurity capabilities rather than in information technology budgets.

Keywords: Risk Management Strategies, Cybersecurity Threats, Threat Mitigation, Fintech, Deterrence Theory, Resource-Based View, Nairobi

JEL Codes: G23, G32, K24, M15, O33, O55

©2026 by the Authors. This Article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>)

INTRODUCTION

Financial technology (fintech) refers to the application of innovative technology to deliver financial services more efficiently, accessibly and conveniently than traditional institutions, and spans mobile payments, digital lending, digital wallets, wealth platforms and blockchain-based services (Lee & Shin, 2018; Nicoletti, 2021). The same digital dependence that drives the sector's growth has made it a prime target for cybercrime. Financial services are among the most attacked sectors globally (Cremer et al., 2022), and cyber-attacks escalated sharply as financial activity moved online during the COVID-19 pandemic (Lallie et al., 2021). In Africa, the financial sector carries a disproportionate share of attacks, and many organisations report recent incidents or unresolved vulnerabilities (Foya & Garikayi, 2021; Mwangi et al., 2022). Cybersecurity threats are therefore not isolated technical problems but strategic risks that affect service continuity, financial stability and customer trust.

Kenya's fintech sector is internationally recognised for advancing financial inclusion through mobile money and digital credit, with Nairobi as its operational hub (Van Cooten & Blythin-Hammond, 2017). The sector is, however, highly tiered. At one end are nationally systemic mobile-money and bank-linked platforms that process very large daily transaction volumes; at the other are early-stage lenders, savings applications and crypto-asset start-ups operating with a handful of staff. The growth of mobile and internet channels has widened the attack surface across both tiers (Chetalam, 2018; Mwangi et al., 2022).

Organisations respond to these threats through cybersecurity risk management, a cycle of identifying, assessing and treating risks (Aven, 2016; Hopkin, 2018). In practice, risk management strategies operate at three mutually reinforcing levels. Technical controls, such as firewalls, encryption, multi-factor authentication, network segmentation, endpoint detection and patch management, raise the cost and difficulty of an attack (Almomani, 2020; Kaur et al., 2021). Governance mechanisms, including documented policies, structured risk identification and assessment, risk prioritisation, incident response planning and regulatory compliance, determine how consistently controls are selected, resourced and reviewed (Giudici, 2018; Hasan & Hoque, 2023). Human-factor measures, chiefly security awareness training and phishing simulation, address the social-engineering vectors that technical controls cannot close on their own (Parsons et al., 2014).

The effectiveness of risk management depends on how these levels are integrated rather than on any single measure. Awareness training without technical enforcement erodes as attackers change tactics; technical controls without governance decay through misconfiguration and delayed patching; and governance documents without the capability to act on them become compliance exercises (Kristian et al., 2024). How Nairobi's fintech companies combine these strategies, and whether the combination measurably mitigates threats, is the focus of this study.

Statement of the Problem

Kenya's exposure to cyber threats has grown rapidly. The Communications Authority of Kenya detected about 2.54 billion cyber threat events between January and March 2025 and 4.59 billion between April and June 2025, an increase of 80.7% within a single quarter (Communications Authority of Kenya [CA], 2025). In the banking sector, which is closely interconnected with fintech platforms, reported cyber fraud cases rose from 173 in 2023 to 353 in 2024, while losses grew from KSh 412 million to KSh 1.59 billion (Central Bank of Kenya [CBK], 2025). Nairobi, which hosts the highest concentration of fintech firms, transaction volumes and cybersecurity decision-makers, is at the centre of this exposure.

Most fintech companies have adopted some cybersecurity controls, yet incidents and losses continue to rise. Three structural conditions explain why existing controls fall short. First, capital and skills constraints mean that many young firms cannot afford dedicated security staff, a security operations centre or regular penetration testing, so security is often handled by general IT staff. Second, the regulatory perimeter is fragmented. Banks, payment service providers, digital credit providers and virtual asset service providers fall under different instruments (CBK, 2017, 2019; Republic of Kenya, 2019, 2025; Central Bank of Kenya (Digital Credit Providers) Regulations, 2022), leaving uneven baseline requirements and enforcement across fintech categories (Musamali et al., 2024; Juma & Faturoti, 2025). Third, there is a structural mismatch between inherited banking risk frameworks and agile fintech operations. Annual risk cycles, periodic audits and perimeter-based controls were designed for relatively stable banking systems, whereas fintech firms release software continuously and depend on application programming interfaces (APIs), cloud services and third-party integrations, so their attack surface changes faster than periodic assessment can follow (Grima et al., 2023; Javaheri et al., 2023).

The result is a widening conflict between the rising sophistication of attackers and a defensive posture among Nairobi's fintech companies that remains largely periodic, compliance-driven and reactive. What remains unknown is whether, and how strongly, the risk management strategies these firms actually use translate into measurable mitigation outcomes, and where they fall short. Without this evidence, fintech managers cannot prioritise scarce security resources and regulators cannot design proportionate standards. This study addressed that gap.

Objectives of the Study

The broad objective was to examine the effect of risk management strategies on the mitigation of cybersecurity threats in fintech companies in Nairobi City, Kenya. The specific objectives were to:

- i. identify the cybersecurity threats faced by fintech companies in Nairobi City;
- ii. assess the types and levels of risk management strategies employed by fintech companies in Nairobi City; and
- iii. determine the effect of risk management strategies on the mitigation of cybersecurity threats in fintech companies in Nairobi City.

LITERATURE REVIEW

Theoretical Review

Deterrence Theory

Deterrence Theory holds that offending can be discouraged by raising the perceived certainty, severity and swiftness of sanctions, because potential offenders weigh expected benefits against expected costs. The theory was carried into information systems security by Straub (1990) and later applied to user security behaviour (Ng & Rahim, 2005). In cybersecurity, deterrence operates through the certainty of detection and the severity of consequences, which access controls, monitoring, audit trails and administrative safeguards are designed to raise (Willison & Warkentin, 2013). Applied to this study, the theory explains how risk identification, assessment and mitigation can make malware, phishing and DDoS attacks harder to execute and easier to detect. For example, multi-factor authentication raises the effort needed to exploit stolen credentials, while traffic filtering and real-time monitoring increase the likelihood of detecting and disrupting a DDoS attack.

The theory has an important limitation in this setting. It originated in explaining rational criminal behaviour in physical contexts and, within organisations, employee compliance with security policy (Willison & Warkentin, 2013). Most attacks on fintech platforms come instead from external, distributed and often anonymous actors, such as ransomware syndicates, cross-border fraud groups and automated botnets. Attribution in cyberspace is slow and uncertain (Rid & Buchanan, 2015), many offenders operate beyond the practical reach of Kenya's Computer Misuse and Cybercrimes Act (Republic of Kenya, 2018), and a botnet executing a DDoS attack makes no calculation about punishment at all. The assumption that attackers rationally weigh the certainty, severity and swiftness of punishment in Kenya's jurisdiction is therefore weak. Nye (2017) argues that in cyberspace, deterrence by denial, which makes attacks less likely to succeed, is more feasible than deterrence by punishment. This study accordingly applies Deterrence Theory mainly in its denial form: technical friction that lowers an attacker's expected payoff matters more for mitigation than the prospect of legal sanction, which remains relevant chiefly for insiders and locally based fraud networks.

Resource-Based View and Dynamic Cybersecurity Capabilities

The Resource-Based View (RBV) holds that organisations gain sustained advantage from resources that are valuable, rare, inimitable and non-substitutable (Barney, 1991). Applied loosely, RBV risks becoming a tautology, in which firms with more resources perform better because they have more resources (Kraaijenbrink et al., 2010). To avoid this, the study ties RBV specifically to dynamic cybersecurity capabilities: the organisational ability to integrate, build and reconfigure security competencies as threats change (Teece et al., 1997). In cybersecurity these capabilities take concrete forms, including specialised human capital such as security analysts and Chief Information Security Officers, threat intelligence routines, continuous vulnerability management, tested incident response playbooks and real-time security analytics (Naseer et al., 2021). Such capabilities are hard to imitate because they are built through practice and accumulated experience rather than purchased. A large IT budget spent on tools without the routines and people to operate them does not confer advantage.

This framing shaped the measurement of the independent variable, which captures security routines (vulnerability assessment, threat intelligence, risk prioritisation and impact quantification) rather than security spending. The two theories are complementary. Deterrence Theory explains what effective controls do to attackers, by raising friction and the probability of detection, while RBV explains why fintech firms differ in their ability to build and sustain those controls.

Empirical Review

Cybersecurity Threats Facing Fintech Companies

A systematic review by Javaheri et al. (2023) identifies malware, phishing and DDoS attacks as the core threats to fintech infrastructure, each exploiting a different feature of the fintech model. Malware, particularly ransomware and cryptojacking, targets the high-value, always-on transaction environment; Kaur et al. (2021) report ransomware as the most damaging variant, and Spelman (2022) shows that machine-learning detection outperforms signature-based antivirus against such threats. Phishing exploits the digital communication channels on which fintech depends, and has evolved into spear-phishing and SMS-based smishing that target mobile users directly (Javaheri et al., 2023; AlBenJasim et al., 2023). Employee susceptibility remains high even in organisations with awareness programmes (Parsons et al., 2014). DDoS attacks target availability, causing service outages and eroding customer trust,

and their effective mitigation requires detection infrastructure that many organisations lack (Chaganti et al., 2022).

Integration with partners compounds these threats. Najaf et al. (2020) show that collaborative fintech–bank platforms widen the attack surface because a compromise in one partner can propagate to others. Much of this evidence, however, comes from mature markets with stronger security investment and enforcement (Cremer et al., 2022). In Nairobi, mobile-first delivery, high volumes of mobile-money transactions and uneven digital literacy are likely to shift the balance of threats, for example towards SMS and social-media phishing, in ways that global studies do not capture (Chetalam, 2018; Mwangi et al., 2022).

Risk Management Strategies Employed by Fintech Companies

Structured risk identification, including system audits, vulnerability assessments, penetration testing and threat monitoring, enables organisations to detect more threats than ad hoc approaches (Hasan & Hoque, 2023), and failures at this stage propagate through the whole risk management process (Giudici, 2018). For risk assessment, quantitative techniques such as risk scoring and impact analysis improve prioritisation (Demyanova, 2018), and adaptive frameworks that reassess risk continuously outperform static ones in fast-changing fintech environments (Sapian et al., 2020). Mitigation relies on layered technical, organisational and human controls (Kristian et al., 2024), supported by analytics-driven monitoring (Chowdhury & Kulkarni, 2023). Persistent weaknesses include delayed patching driven by resource constraints and fears of operational disruption (Almomani, 2020).

In Nairobi, firm tier determines how these strategies work in practice. Tier-1 providers, such as the mobile-money and bank-linked platforms in the M-Pesa ecosystem, are supervised as payment service providers and are expected to maintain board-level cybersecurity governance, continuous monitoring and independent testing (CBK, 2019). Their main difficulty in identifying risks is scale and complexity: extensive agent networks, partner APIs and third-party integrations create exposures that no single assessment can cover. Tier-3 micro-fintech start-ups, by contrast, often lack the asset inventories, logging and dedicated staff needed to know what must be protected, and depend on cloud defaults, outsourced developers and occasional scans. A uniform identification framework therefore fails both groups. A bank-style checklist under-specifies the ecosystem and third-party risks of Tier-1 providers, while for Tier-3 firms it is unaffordable, so they default to compliance on paper. This is why proportionate, risk-based supervision has been advocated for fintech (Bains & Wu, 2023).

Risk Management and the Mitigation of Cybersecurity Threats

Mitigation is reflected in reduced financial fraud losses, fewer cybersecurity incidents and lower perceived risk exposure. On fraud losses, machine-learning and AI-driven frameworks improve fraud prevention in financial transactions (Bello et al., 2023), and proactive financial cybersecurity risk management systems have been found to reduce losses in Nigerian banking payment systems (Otuu & Aguboshim, 2023). This evidence comes mainly from commercial banking, however, and cannot be transferred directly to fintech. Fintech fraud vectors differ in kind. Open and partner APIs are exposed to broken object-level authorisation, broken authentication and abuse of business flows (OWASP Foundation, 2023). App-based wallets are vulnerable to device compromise, credential stuffing and social engineering through mobile channels. Decentralised, cloud-native technology stacks spread control across many third-party providers, so that a compromise at one vendor can cascade (Javaheri et al., 2023; Najaf et al.,

2020). Fraud-detection models built on card, branch and wire-transfer patterns therefore cannot be assumed to perform equally well against these vectors.

On incident frequency, layered approaches that cover prevention, detection, response and recovery substantially reduce successful attacks (Kristian et al., 2024). On perceptions, structured risk management improves stakeholder assessments of security posture and sector resilience (Mwase et al., 2024), and dynamic capabilities strengthen organisational confidence in handling threats (Pigola & da Costa, 2025). These relationships are also conditioned by the external environment. Strong regulation is associated with more comprehensive controls (Atere, 2022), central-bank oversight sets baseline standards (Rajaiah et al., 2022), and Kenya's overlapping supervisory mandates make the coherence of oversight an open question (Musamali et al., 2024).

Research Gap

Taken together, the literature leaves three gaps that this study addresses. The first is contextual: evidence on the threat–strategy–outcome relationship comes predominantly from mature markets and from banks rather than from fintech firms in sub-Saharan Africa. The second concerns heterogeneity: prior studies rarely consider how firm tier, staffing and resources shape the quality of risk management. The third is architectural: findings from banking are routinely applied to fintech despite fundamentally different technology stacks and fraud vectors. Little locally grounded quantitative evidence exists on the extent to which risk management strategies explain mitigation outcomes in Nairobi's fintech sector.

Conceptual Framework

Figure 1 presents the conceptual framework. Cybersecurity threats (malware, phishing and DDoS attacks) and risk management strategies (identification, assessment and mitigation practices) are the independent variables. Mitigation of cybersecurity threats, measured through reduced fraud losses, fewer incidents and lower risk exposure perceptions, is the dependent variable. Government regulations, compliance authorities and external market factors are intervening variables that may strengthen or weaken these relationships.

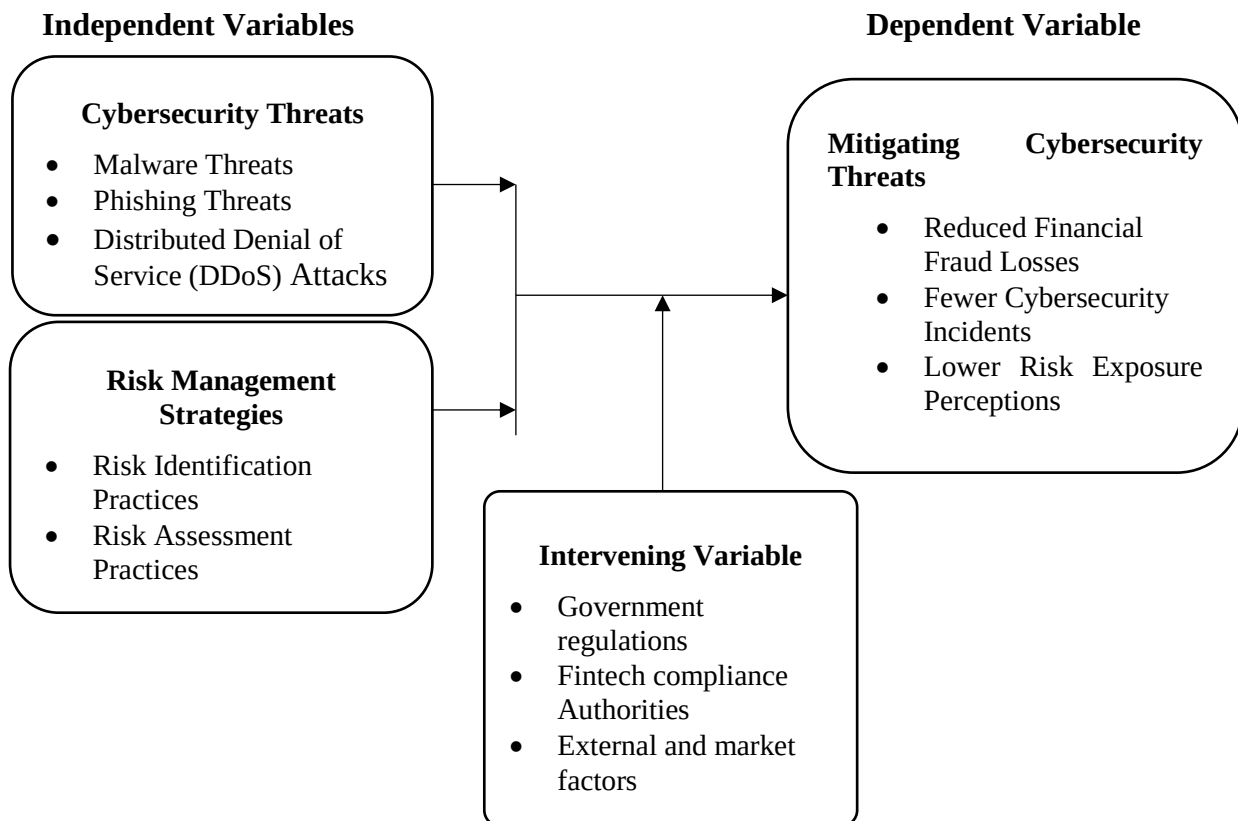


Figure 1: Conceptual Framework

METHODOLOGY

The study adopted a correlational research design, which allows the strength and direction of relationships among variables to be examined without manipulation (Creswell, 2014). It was conducted in Nairobi City because the targeted fintech companies were registered, headquartered and managed there, and their cybersecurity decision-makers were based in the city. The unit of analysis was therefore the organisational practices adopted at headquarters level. The target population comprised 306 professionals responsible for cybersecurity and risk management in the 98 registered fintech companies operating in Nairobi City, estimated from the number of relevant staff in each size category. Yamane's (1967) formula, $n = N / [1 + N(e^2)]$, with $N = 306$ and $e = 0.05$, gave a sample of 173 respondents, who were allocated proportionately across strata and then selected by simple random sampling (Table 1). In addition, 12 key informants, including Chief Information Security Officers (CISOs), heads of IT and risk and compliance managers, were selected purposively.

Primary data were collected using a structured questionnaire and a key informant interview guide. The questionnaire comprised four sections: demographics; cybersecurity threats; risk management practices; and mitigation outcomes. Each construct was measured by six items on a five-point Likert scale (1 = strongly disagree, 5 = strongly agree), complemented by open-ended questions. Questionnaires were administered through a drop-and-pick-later method with follow-up by email and telephone. Interviews lasted 45 to 60 minutes, and informants were coded R01 to R12. A pilot study with eight respondents (about 5% of the sample) from large, medium and small fintech firms in Nakuru County tested the instruments and was excluded from the main study. Content validity was established through review by a panel of five

experts: three academics in cybersecurity and information systems and two fintech risk practitioners. Face validity was established through pilot feedback, and construct validity through the Kaiser-Meyer-Olkin measure, Bartlett's Test of Sphericity and exploratory factor analysis (Hair et al., 2019). Internal consistency was assessed using Cronbach's alpha against a threshold of 0.70.

Quantitative data were analysed in SPSS Version 30. Composite indices were computed as the mean of each construct's six items, and descriptive statistics, Pearson correlation and ordinary least squares regression were applied. Three models were estimated, where Y is mitigation of cybersecurity threats, X_1 is risk management strategies, X_2 is cybersecurity threats and ε is the error term:

$$\text{Model 1: } Y = \beta_0 + \beta_1 X_1 + \varepsilon$$

$$\text{Model 2: } Y = \beta_0 + \beta_2 X_2 + \varepsilon$$

$$\text{Model 3: } Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \varepsilon$$

Qualitative data were transcribed, coded against the study objectives and analysed thematically to explain the quantitative results. Ethical approval was obtained from Egerton University and a research permit from the National Commission for Science, Technology and Innovation (NACOSTI). Participation was voluntary and based on informed consent, responses were anonymised, and respondents were not asked to disclose proprietary security details.

FINDINGS AND DISCUSSION

Response Rate and Respondent Profile

Of the 173 questionnaires administered, 145 were returned and usable, a response rate of 83.8%, which exceeds the 50% considered adequate for analysis (Mugenda & Mugenda, 2003). All 12 key informant interviews were completed. As Table 2 shows, IT managers formed the largest group of respondents (35.9%), reflecting the fact that in many smaller firms IT staff also carry cybersecurity responsibilities, whereas CISOs made up only 6.2%. Most respondents worked in medium enterprises (62.1%), in mobile banking and payments (36.6%), and in firms that had operated for two to five years (38.6%). Respondents self-classified their firms using the questionnaire's size bands, which differ from the staffing-based strata used for sampling, so the two distributions are not directly comparable.

Table 1: Profile of Respondents (n = 145)

Characteristic	Category	Frequency	Percent
Professional role	IT managers	52	35.9
	Risk managers	38	26.2
	Cybersecurity managers	27	18.6
	Compliance officers	19	13.1
	Chief Information Security Officers	9	6.2
Company category	Small enterprise (2–10 employees)	39	26.9
	Medium enterprise (11–50 employees)	90	62.1
	Established company (50+ employees)	16	11.0
Primary service	Mobile banking/payments	53	36.6
	Lending	42	29.0
	Wealth management	33	22.8
	Cryptocurrencies	17	11.7
Years of operation	Less than 2 years	27	18.6
	2–5 years	56	38.6
	6–10 years	41	28.3
	More than 10 years	21	14.5

Cybersecurity Threats Faced by Fintech Companies**Table 2: Cybersecurity Threats Faced by Fintech Companies (n = 145)**

Statement	Mean	SD
Our systems have been affected by malware infections, such as viruses, worms, or ransomware attacks	4.57	0.524
Malware infections have resulted in data loss or system downtime within our organisation	3.99	1.003
Our organisation has experienced phishing attempts aimed at stealing sensitive information or credentials	3.46	1.318
Phishing attacks have led to unauthorised access or data breaches within our systems	3.41	1.256
Our organisation has been targeted by DDoS attacks that overwhelmed our systems and caused service disruptions	3.41	1.326
DDoS attacks have resulted in financial losses or reputational damage for our organisation	3.91	1.317

Table 2 shows that malware infections were the most prevalent threat ($M = 4.57$) and the item with the lowest dispersion ($SD = 0.524$), indicating consensus across firm sizes and service types. Respondents also agreed that malware had caused data loss or downtime ($M = 3.99$). About 52% of respondents reported a major malware incident in the previous three years. Key informants described “a ransomware attack [that] encrypted several file servers, disrupting operations for two days” (R08) and “a ransomware incident [that] led to partial data loss and required system restoration from backups” (R05). Phishing was moderately prevalent ($M = 3.46$), but its high dispersion ($SD = 1.318$) suggests that exposure depends on each firm’s level of awareness and email filtering. Email remained the main vector, yet informants also reported that “SMS phishing is the most frequently observed” (R05) and that social-media phishing was common (R01). Business email compromise was singled out as especially dangerous “due to direct financial fraud potential” (R01). DDoS attacks were less frequent ($M = 3.41$), but their

financial and reputational consequences were rated severely ($M = 3.91$), showing that DDoS attacks are infrequent but highly damaging when they occur.

These results agree with Javaheri et al. (2023) and Kaur et al. (2021) in placing malware, and ransomware in particular, at the centre of fintech risk. They extend that literature in two ways. First, phishing in Nairobi is migrating to SMS and social-media channels, consistent with the mobile-first fintech model (Chetalam, 2018). Second, the severity of DDoS consequences relative to their frequency suggests that many firms lack the traffic-filtering and monitoring capacity identified by Chaganti et al. (2022).

Risk Management Strategies Employed by Fintech Companies

Table 3: Risk Management Strategies Employed by Fintech Companies (n = 145)

Statement	Mean	SD
Our organisation conducts regular vulnerability assessments to identify potential cybersecurity risks	3.83	1.202
We gather and analyse threat intelligence from various sources to identify emerging cybersecurity threats	3.79	1.237
We prioritise identified risks based on their likelihood of occurrence and potential impact	3.73	1.180
Our risk assessment process quantifies the potential financial and reputational consequences of cyber threats	3.70	1.161
We implement technical controls, such as firewalls, encryption, and access controls, to mitigate cybersecurity risks	3.52	1.275
Our organisation has comprehensive cybersecurity policies and procedures to guide risk mitigation efforts	3.81	1.298

Table 3 shows that risk management practices were implemented at a moderate level. Vulnerability assessments ($M = 3.83$), comprehensive policies ($M = 3.81$) and threat intelligence gathering ($M = 3.79$) scored highest, followed by risk prioritisation ($M = 3.73$) and impact quantification ($M = 3.70$). Technical controls recorded the lowest mean ($M = 3.52$) and high dispersion ($SD = 1.275$). Standard deviations above 1.16 for every item point to marked differences in risk management maturity across firms. The qualitative data show where this variation comes from. About 58% of respondents reported having dedicated cybersecurity roles, such as CISOs, information security managers and cyber risk managers, whereas 42% did not. In the latter firms, “cybersecurity is managed on an ad hoc basis” (R07), “risk management is outsourced” (R06), or responsibilities fall to general IT staff. Assessment practices ranged from “an external vulnerability scan ... on internet-facing systems” (R01) to “a full-scope penetration test cover[ing] network, application, and cloud infrastructure” (R04). Informants identified the least effective practices as annual assessments that “do not reflect rapidly changing threats” (R01), “manual risk tracking [that] causes delays and human error” (R02), “checkbox compliance exercises [that] lack real risk insight” (R03), and “overreliance on policies without enforcement or monitoring” (R08).

These findings support Hasan and Hoque (2023) on the value of structured identification, but they also show the tier divide described in Section 2.2.2. Policies scored higher than technical controls, which suggests that some firms document security more readily than they implement it. This pattern matches the mismatch between periodic, document-centred frameworks and continuously changing fintech systems (Sapian et al., 2020). The 42% of firms without

dedicated security roles, together with the weakness of technical controls, also reflects the patching and resourcing constraints reported by Almomani (2020).

Mitigation of Cybersecurity Threats

Table 4: Mitigation of Cybersecurity Threats

Statement	Mean	SD
Our risk management practices have contributed to reducing financial losses resulting from cybersecurity-related fraud	3.88	1.228
Effective risk management has minimised the financial impact of cyber threats on our organisation	3.31	1.446
The number of cybersecurity incidents we have experienced has decreased due to our risk management efforts	3.77	1.123
Our risk management strategies have effectively prevented or mitigated various types of cybersecurity incidents	3.69	1.109
Our stakeholders (customers, partners, regulators) perceive our organisation as having lower exposure to cybersecurity risks	3.70	1.155
Our risk management practices have improved the perception of our organisation's cybersecurity posture	4.04	1.066

As Table 4 shows, improved perception of cybersecurity posture received the highest rating ($M = 4.04$, $SD = 1.066$), followed by reduction of fraud losses ($M = 3.88$) and fewer incidents ($M = 3.77$). Minimisation of the overall financial impact of cyber threats scored lowest and varied most ($M = 3.31$, $SD = 1.446$). Informants gave concrete examples of successful mitigation: “MFA prevented attacker access after stolen credentials were detected” (R03), “network segmentation limited malware spread to a single workstation” (R04), and “a ransomware attack was contained because offline backups were regularly tested” (R02). Multi-factor authentication, awareness training, patch management, segmentation and endpoint detection and response were cited most often as the measures with the greatest effect. Persistent gaps included inconsistent awareness across departments, immature incident response, weak third-party risk management, limited continuous monitoring and slow remediation. The difference between the perception score and the financial-impact score points to a perception protection gap. Firms appear more successful at signalling security competence through certifications, documented policies and transparent communication (“customers are reassured by our security certifications”, R12) than at consistently reducing financial losses. This finding qualifies the positive perception effects reported by Mwase et al. (2024). It also suggests that the bank-derived fraud controls discussed by Otuu and Aguboshim (2023) do not yet translate fully to fintech-specific fraud vectors.

Correlation Analysis

Table 5: Pearson Correlation Matrix

Variable	1	2	3
1. Mitigation of cybersecurity threats	1.000		
2. Cybersecurity threats	.622**	1.000	
3. Risk management practices	.705**	.608**	1.000

Table 5 shows that all relationships were positive and significant at the 0.01 level. Risk management practices had the strongest association with mitigation ($r = .705$), followed by

cybersecurity threats ($r = .622$). The positive correlation between threats and risk management ($r = .608$) suggests a reactive pattern, in which firms facing greater exposure invest more in risk management.

Regression Analysis

Table 6: Regression of Mitigation on Risk Management Practices and Cybersecurity Threats

Predictor / Statistic	Model 1	Model 2	Model 3
Constant	1.121 (0.221) $t = 5.082^{***}$	1.334 (0.254) $t = 5.254^{***}$	0.630 (0.237) $t = 2.661^{**}$
Risk management practices (X_1)	0.720 (0.060) $\beta = .705, t = 11.900^{***}$	—	0.530 (0.072) $\beta = .519, t = 7.378^{***}$
Cybersecurity threats (X_2)	—	0.617 (0.065) $\beta = .622, t = 9.488^{***}$	0.303 (0.070) $\beta = .306, t = 4.340^{***}$
R	.705	.622	.746
R ²	.498	.386	.556
Adjusted R ²	.494	.382	.550
Std. error of estimate	.26921	.29751	.25384
F (df)	141.604 (1, 143) ^{***}	90.031 (1, 143) ^{***}	89.050 (2, 142) ^{***}

Model 1 (Table 6) shows that risk management practices significantly predicted mitigation ($F = 141.604, p < .01$), explaining 49.8% of its variance. A one-unit increase in risk management practices was associated with a 0.720-unit increase in mitigation ($\beta = .705, t = 11.900$). Model 2 shows that threat exposure alone explained 38.6% of the variance ($F = 90.031, p < .01$). In the combined Model 3 ($F = 89.050, p < .01$; $R^2 = .556$), both predictors remained significant, but risk management had the larger unique contribution ($\beta = .519, t = 7.378$) compared with threats ($\beta = .306, t = 4.340$). Adding threats to Model 1 raised the explained variance by 5.8 percentage points. The correlation between the two predictors ($r = .608$) implies a variance inflation factor of about 1.59, well below conventional thresholds, so multicollinearity was not a concern (Hair et al., 2019). The fitted equation is:

$$Y = 0.630 + 0.530X_1 + 0.303X_2$$

The positive coefficient for threats should not be read as threats “causing” mitigation. It more plausibly reflects reactive investment, as firms that have been attacked strengthen their defences and report the gains. Because the design is correlational and threats, practices and outcomes were reported by the same respondents, the coefficients are interpreted as associations rather than strict causal effects.

Discussion

The results support the study’s theoretical framing with the qualifications. Consistent with deterrence by denial (Nye, 2017), the measures informants credited with the greatest effect (multi-factor authentication, segmentation, endpoint detection and tested backups) all raise technical friction or limit the damage of an attack, rather than relying on legal sanction against attackers who are mostly beyond local jurisdiction. Consistent with a capability-based reading of RBV (Teece et al., 1997; Naseer et al., 2021), the strongest predictor of mitigation was a set of security routines rather than spending. The weakest areas, namely continuous monitoring, incident response maturity and remediation speed, are precisely the dynamic capabilities that firms without dedicated security staff cannot easily build. The findings converge with Kristian et al. (2024) on the benefits of layered risk management. They extend that work by showing that in Nairobi the relationship is shaped by firm tier, by a perception–protection gap, and by

fintech-specific threat channels. The 44.4% of variance left unexplained in Model 3 indicates that other factors, such as security culture, leadership commitment and regulatory enforcement, also matter.

CONCLUSION AND RECOMMENDATIONS

Conclusion

First, fintech companies in Nairobi City face a threat landscape dominated by malware, especially ransomware, together with phishing that is increasingly delivered through SMS and social media, and DDoS attacks that are infrequent but highly damaging. Defences must therefore address both technical vulnerabilities and human attack pathways. Second, risk management strategies are implemented at a moderate level, with vulnerability assessments and threat intelligence most common and technical controls least developed. Maturity is uneven, and the 42% of firms without dedicated security roles form a lower tier that relies on periodic, document-centred practice. Third, risk management strategies have a significant positive association with the mitigation of cybersecurity threats, explaining nearly half of the variation in outcomes. Mitigation remains uneven, however, and firms are better at improving their security reputation than at reducing the financial impact of attacks.

Recommendations

Practice. Fintech companies should: (i) enforce multi-factor authentication on all user and administrative accounts; (ii) replace annual assessments with continuous, automated vulnerability scanning and monitoring; (iii) run role-based awareness training with regular phishing simulations that cover SMS and social-media vectors; (iv) appoint dedicated cybersecurity personnel proportionate to their size and risk, such as an information security officer in medium firms and a security operations function in large ones; (v) deploy layered controls, including segmentation, endpoint detection and response, timely patching and tested offline backups; and (vi) maintain incident response playbooks validated through tabletop exercises.

Policy. The Central Bank of Kenya, the Communications Authority of Kenya and related regulators should: (i) harmonise the existing fragmented instruments into proportionate minimum cybersecurity standards that cover all fintech categories, including digital lenders and virtual asset service providers; (ii) mandate independent security audits that test the effectiveness of controls, not only their documentation, for firms above defined transaction or customer thresholds; (iii) operationalise sector-wide threat intelligence sharing and anonymous incident reporting through the national computer incident response team; and (iv) offer incentives such as grants or preferential regulatory treatment for certified security programmes, prioritising small and medium firms.

Theory. The study refines both theories for fintech cybersecurity. Deterrence operates mainly through denial rather than punishment, and resource-based advantage arises from dynamic cybersecurity capabilities rather than from IT budgets. Future applications of both theories in this field should specify these boundary conditions explicitly.

Limitations and Suggestions for Further Research

The cross-sectional, single-source design limits causal inference and may inflate associations through common-method variance, and the study was confined to Nairobi. Future research should use longitudinal and multi-source data, including objective incident and loss records,

compare fintech tiers and other Kenyan cities, quantify the costs of incidents to support cost–benefit analysis of controls, and test the moderating role of regulation empirically.

REFERENCES

- AlBenJasim, S., Dargahi, T., Takturi, H., & Al-Zaidi, R. (2023). FinTech cybersecurity challenges and regulations: Bahrain case study. *Journal of Computer Information Systems*, 1–17. <https://doi.org/10.1080/08874417.2023.2187394>
- Almomani, A. (2020). Cyber security attacks: A review of common types, prevention, and detection. *Journal of Information Security*, 11(4), 251–266. <https://doi.org/10.4236/jis.2020.114016>
- Atere, T. O. (2022). *Cybersecurity regulation in the financial sector: Reflexive risk management in the UK, USA and Nigeria* [Doctoral dissertation, Newcastle University].
- Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, 253(1), 1–13. <https://doi.org/10.1016/j.ejor.2015.12.023>
- Bains, P., & Wu, C. (2023). *Institutional arrangements for fintech regulation: Supervisory monitoring* (Fintech Note). International Monetary Fund. <https://doi.org/10.5089/9798400234058.001>
- Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, 17(1), 99–120. <https://doi.org/10.1177/014920639101700108>
- Bello, O. A., Folorunso, A., Ejiofor, O. E., Budale, F. Z., Adebayo, K., & Babatunde, O. A. (2023). Machine learning approaches for enhancing fraud prevention in financial transactions. *International Journal of Management Technology*, 10(1), 85–108.
- Central Bank of Kenya (Digital Credit Providers) Regulations, Legal Notice No. 46 of 2022. (2022). Government Printer.
- Central Bank of Kenya. (2017). *Guidance note on cybersecurity*. Central Bank of Kenya.
- Central Bank of Kenya. (2019). *Guideline on cybersecurity for payment service providers*. Central Bank of Kenya.
- Central Bank of Kenya. (2025). *Bank supervision annual report 2024*. Central Bank of Kenya.
- Chaganti, R., Bhushan, B., & Ravi, V. (2022). *The role of blockchain in DDoS attacks mitigation: Techniques, open challenges and future directions*. arXiv. <https://doi.org/10.48550/arXiv.2202.03617>
- Chetalam, L. J. (2018). *Enhancing security of MPesa transactions by use of voice biometrics* [Master's thesis, United States International University-Africa].
- Chowdhury, D., & Kulkarni, P. (2023). Application of data analytics in risk management of fintech companies. In *2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA)* (pp. 384–389). IEEE. <https://doi.org/10.1109/ICIDCA56705.2023.10100067>
- Communications Authority of Kenya. (2025). *Cyber security report: Fourth quarter of the financial year 2024/2025 (April–June 2025)*. Communications Authority of Kenya.

- Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance – Issues and Practice*, 47(3), 698–736. <https://doi.org/10.1057/s41288-022-00266-6>
- Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). SAGE.
- Demyanova, E. A. (2018). Current issues of company evaluation under fintech. *Strategic Decisions and Risk Management*, 1, 102–113.
- Foya, D., & Garikayi, V. R. (2021). Assessing cyber security awareness and organisational preparedness on cyber security in audit firms. *Indiana Journal of Economics and Business Management*, 1(1), 19–34.
- Giudici, P. (2018). Fintech risk management: A research challenge for artificial intelligence in finance. *Frontiers in Artificial Intelligence*, 1, 1. <https://doi.org/10.3389/frai.2018.00001>
- Grima, S., Thalassinios, E., Cristea, M., Kadlubek, M., Maditinos, D., & Peiseniece, L. (Eds.). (2023). *Digital transformation, strategic resilience, cyber security and risk management*. Emerald. <https://doi.org/10.1108/9781803826103>
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.). Cengage Learning.
- Hasan, M., & Hoque, A. (2023). FinTech risk management and monitoring. In *Novel financial applications of machine learning and deep learning* (pp. 3–16). Springer. https://doi.org/10.1007/978-3-031-18552-6_1
- Hopkin, P. (2018). *Fundamentals of risk management: Understanding, evaluating and implementing effective risk management* (5th ed.). Kogan Page.
- Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2023). Cybersecurity threats in FinTech: A systematic review. *Expert Systems with Applications*, 122697. <https://doi.org/10.1016/j.eswa.2023.122697>
- Juma, I., & Faturoti, B. (2025). Enforcing data privacy in Kenya and Nigeria: Towards an African approach to regulatory practice. *International Review of Law, Computers & Technology*, 1–26.
- Kaur, G., Habibi Lashkari, Z., & Habibi Lashkari, A. (2021). *Understanding cybersecurity management in FinTech*. Springer. <https://doi.org/10.1007/978-3-030-79915-1>
- Kraaijenbrink, J., Spender, J.-C., & Groen, A. J. (2010). The resource-based view: A review and assessment of its critiques. *Journal of Management*, 36(1), 349–372. <https://doi.org/10.1177/0149206309350775>
- Kristian, A., Az-Zahra, A. R., Hidayat, F., Fauzi, A. Y., & Kallas, E. (2024). Enhancing cybersecurity risk management strategies in financial institutions: A comprehensive analysis of threats and mitigation approaches. *Journal of Computer Science and Technology Application*, 1(2), 96–103. <https://doi.org/10.52909/jcsta.v1i2.178>

- Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, 105, 102248. <https://doi.org/10.1016/j.cose.2021.102248>
- Lee, I., & Shin, Y. J. (2018). Fintech: Ecosystem, business models, investment decisions, and challenges. *Business Horizons*, 61(1), 35–46. <https://doi.org/10.1016/j.bushor.2017.09.003>
- Mugenda, O. M., & Mugenda, A. G. (2003). *Research methods: Quantitative and qualitative approaches*. ACTS Press.
- Musamali, R., Jugurnath, B., Maalu, J., & Mahuni, K. (2024). Fintech regulation in Kenya: Global practises and lessons learnt. *Journal of Smart Economic Growth*, 9(2), 32–66.
- Mwangi, T., Asava, T., & Akerele, I. (2022). Cybersecurity threats in Africa. In *The Palgrave handbook of sustainable peace and security in Africa* (pp. 159–180). Palgrave Macmillan. https://doi.org/10.1007/978-3-030-96462-4_8
- Mwase, A., Ngassam, E. K., & Singh, S. (2024). Fintech resilience: An exploration of security risks and risk management strategies. *Scientific and Practical Cyber Security Journal*. <https://doi.org/10.58254/spcyb.2024.1.15.142>
- Najaf, K., Schinckus, C., Mostafiz, M. I., & Najaf, R. (2020). Conceptualising cybersecurity risk of fintech firms and banks sustainability. *International Journal of Financial Innovation in Banking*. <https://doi.org/10.1504/IJFIB.2020.108767>
- Naseer, H., Maynard, S. B., & Desouza, K. C. (2021). Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis. *International Journal of Information Management*, 59, 102334. <https://doi.org/10.1016/j.ijinfomgt.2021.102334>
- Ng, B. Y., & Rahim, M. A. (2005). A socio-behavioral study of home computer users' intention to practice security. In *Proceedings of the Pacific Asia Conference on Information Systems (PACIS 2005)* (pp. 234–247).
- Nicoletti, B. (2021). *Banking 5.0: How fintech will change traditional banks in the 'new normal' post pandemic*. Palgrave Macmillan. <https://doi.org/10.1007/978-3-030-75871-4>
- Nye, J. S., Jr. (2017). Deterrence and dissuasion in cyberspace. *International Security*, 41(3), 44–71. https://doi.org/10.1162/ISEC_a_00266
- Otuu, O. O., & Aguboshim, F. C. (2023). Exploring the role of financial cybersecurity risk management in enhancing the performance of banking payment systems in Nigeria: A qualitative case study. In *2023 IEEE International Humanitarian Technology Conference (IHTC)* (pp. 1–8). IEEE. <https://doi.org/10.1109/IHTC58054.2023.10366147>
- OWASP Foundation. (2023). OWASP API security top 10 – 2023. <https://owasp.org/API-Security/editions/2023/en/0x11-t10/>

- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42, 165–176.
<https://doi.org/10.1016/j.cose.2013.12.003>
- Pigola, A., & da Costa, P. R. (2025). Cybersecurity management: An empirical analysis of dynamic capabilities framework for enhancing cybersecurity intelligence. *Information & Computer Security*. <https://doi.org/10.1108/ICS-08-2024-0185>
- Rajaiah, J., Majumder, A., Ingale, K., & Pasumarti, S. S. (2022). Central bank and fintech: Regulatory challenges and framework. In *Digitalization and the future of financial services* (pp. 41–65). Springer.
- Republic of Kenya. (2018). *Computer Misuse and Cybercrimes Act, No. 5 of 2018*. Government Printer.
- Republic of Kenya. (2019). *Data Protection Act, No. 24 of 2019*. Government Printer.
- Republic of Kenya. (2025). *Virtual Asset Service Providers Act, No. 20 of 2025*. Government Printer.
- Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, 38(1–2), 4–37. <https://doi.org/10.1080/01402390.2014.977382>
- Sapian, S. M., Ibrahim, N., & Shahwan, S. H. (2020). The conduct of risk management in trade financing processes: Exploring the prospects and challenges in fintech era. *Humanities & Social Sciences Reviews*, 8(3), 1072–1080. <https://doi.org/10.18510/hssr.2020.83107>
- Spelman, F. (2022). *Predictive analytics for malware detection in FinTech using machine learning classification* [Master's applied research project, Dublin Business School].
- Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, 1(3), 255–276. <https://doi.org/10.1287/isre.1.3.255>
- Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(7), 509–533. [https://doi.org/10.1002/\(SICI\)1097-0266\(199708\)18:7<509::AID-SMJ882>3.0.CO;2-Z](https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z)
- Van Cooten, J., & Blythin-Hammond, J. (2017). *The development of FinTech in Nairobi: Contributions to financial inclusion and barriers to growth*.
- Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, 37(1), 1–20.
<https://doi.org/10.25300/MISQ/2013/37.1.01>
- Yamane, T. (1967). *Statistics: An introductory analysis* (2nd ed.). Harper & Row.