EVALUATING THE EFFECTIVENESS OF CYBERSECURITY FRAMEWORKS IN MITIGATING PHISHING THREATS IN DIGITAL MICROFINANCE INSTITUTIONS

Richard Mathenge, Catherine Mukunga and Ephantus Mwangi

School of Pure and Applied Sciences, Kirinyaga University, Kerugoya, Kenya

ABSTRACT

Phishing remains a dominant cybersecurity threat worldwide, particularly affecting Digital Microfinance Institutions (MFIs) in resource-limited settings. Although the most popular frameworks, including ISO/IEC 27001, NIST CSF, COBIT, and CIS Controls, are widely recognized, their effectiveness in preventing phishing attacks in MFIs remains unexplored. This research follows a qualitative-dominant mixed-methods design, with a primary focus on semi-structured interviews with cybersecurity managers (n=24), a staff survey (n=150), and analysis of phishing incident reports from six MFIs in Nairobi, Kenya. Institutions that implemented cybersecurity systems holistically reported reductions in phishing incidents ranging from 22–35% within the sampled institutions, especially when detection and response systems were actively maintained. In contrast, 83% of MFIs used the frameworks as compliance checklists, with limited training and no real-time monitoring. The semi-structured interviews also indicated that infrastructural limitations, poor governance, and the lack of behavioral awareness further limited the framework's effectiveness. To tackle these challenges, the study presents an Adaptive Cybersecurity Framework combining a modular governance system with a lightweight GRU-based phishing mitigation method, tailored for low-resource environments. The study advances understanding of framework adaptation in developing economies and provides actionable insights for developing robust, human-centered cybersecurity frameworks within digital financial inclusion ecosystems.

KEYWORDS

Phishing attacks, Cybersecurity Frameworks, Digital Microfinance Institutions, Adaptive Cybersecurity, GRU Neural Networks

1. INTRODUCTION

The rapid digitalization of microfinance services has transformed financial inclusion in emerging markets; however, significant gaps remain in technological development and cybersecurity readiness. In Sub-Saharan Africa, platforms such as Kenya's M-Pesa enable Microfinance Institutions (MFIs) to integrate API-based systems to detect fraud. Such structural differences create a specific vulnerability profile: Kenyan MFIs face the risk of API exploitation and Subscriber Identity Module (SIM) swapping.

Phishing persists as the most flexible and widespread cybersecurity threat, exploiting technical vulnerabilities and human behavior through SMS spoofing, fake applications, and region-specific social-engineering tactics. Lack of infrastructure, small IT departments, and inconsistent training programs limit MFIs' cybersecurity maturity relative to that of commercial banks. Unequal

preparedness and insufficient regulatory enforcement were identified in a study by Wang et al. [1], which found that 73% of MFIs lacked incident-response measures.

Although comprehensive cybersecurity frameworks such as ISO/IEC 27001, NIST Cybersecurity Framework, COBIT, PCI-DSS, and CIS Controls are accessible, their adoption within microfinance institutions (MFIs) remains primarily symbolic. Frameworks are often used as compliance checklists, which miss local attack vectors, bandwidth limits, and behavioral factors that shape user vulnerability. The lack of connection underscores the need for context-aware, resilience-oriented cybersecurity strategies that integrate technological and human defense components.

Digital Microfinance Institutions (MFIs) play a significant role in promoting financial inclusion for underserved populations; however, the rapid digitalization of their operations has also increased their vulnerability to advanced phishing attacks that exploit both system and cognitive vulnerabilities. [2], [3]. Such attacks, including SMS and email spoofing schemes, fake agent portals, and others, are especially hazardous in low-resource environments due to limited cybersecurity resources and awareness [4]. According to recent surveys, over 60% of MFIs lack real-time monitoring capabilities and rely on limited or outdated staff training [1], [5]. As a result, phishing attacks are on the rise, undermining institutional credibility and threatening the stability of digital financial ecosystems.

The main problem is that existing cybersecurity frameworks remain mostly focused on compliance and are technologically demanding, with limited adaptation to the sociotechnical ecosystems of MFIs. To address this gap, it is essential to assess their practical effectiveness and develop adaptable, scalable solutions, such as AI-driven phishing detection and a resilience-oriented security culture, to enhance protection in low-resource settings. This study fills the gap by empirically evaluating the effectiveness of widely used cybersecurity frameworks in digital microfinance institutions operating in resource-limited environments.

Drawing on a mixed-methods multiple-case study of MFIs in Nairobi, the research examines how governance structures, human behavioral factors, and contextual infrastructure constraints influence phishing resilience. Based on these insights, the study proposes an adaptive cybersecurity framework that integrates lightweight AI-assisted threat detection, modular governance mechanisms, and behaviorally embedded security practices tailored to the operational realities of digital microfinance ecosystems.

1.1. Research Objectives

1. Identify and categorize predominant forms, frequencies, and delivery mechanisms of phishing attacks targeting MFIs, emphasizing how they exploit infrastructural and human vulnera-bilities.
2. Evaluate the degree of adoption and practical effectiveness of existing cybersecurity frame-works in reducing phishing incidents and improving detection-response outcomes.
3. Examine how organizational structures and human factors jointly influence institutional resi-lience.
4. Design adaptive enhancements to existing frameworks, including lightweight AI-based phishing detection mechanisms such as Gated Recurrent Unit (GRU) models, optimized for low-bandwidth environments.

1.2. Research Questions

1. What are the dominant forms, delivery channels, and contextual features of phishing attacks targeting digital MFIs?
2. To what extent do existing cybersecurity frameworks reduce phishing incidents and enhance detection and response in MFIs?
3. How do governance structures and human behavioral factors collectively affect institutional resilience against phishing?
4. What adaptive, AI-supported mechanisms can be embedded in existing frameworks to streng-then phishing detection and response in constrained environments?

2. LITERATURE REVIEW

2.1. Cybersecurity Frameworks in Financial Institutions

Cybersecurity frameworks provide well-organized systems for handling digital threats and enhancing resilience. The most well-known are ISO/IEC 27001, the NIST Cybersecurity Framework (CSF), COBIT, PCI-DSS, and the CIS Controls, which have strengthened governance in the commercial banking sector [6], [7]. However, their applicability to digital microfinance institutions (MFIs) is limited by differences in infrastructure, culture, and resources.

ISO/IEC 27001 is a well-established risk-based information security management framework, but it demands documentation, audits, and leadership engagement, which are often impractical for small MFIs. The five foundational functions of NIST CSF, which are Identify, Protect, Detect, Respond, and Recover, presuppose centralized logging and real-time monitoring [8], capabilities not available to many MFIs. COBIT focuses on congruence in IT governance [9], whereas CIS Controls offer practical configurations [10] that rely on expensive automation tools. Beyond the widely adopted frameworks discussed above, several additional cybersecurity standards are particularly relevant to financial institutions. The Payment Card Industry Data Security Standard (PCI-DSS) provides a comprehensive set of security controls to protect payment systems and cardholder data in financial transactions. Similarly, the National Institute of Standards and Technology Special Publication 800-53 (NIST SP 800-53) provides an extensive catalog of technical security controls that cover system monitoring, identity management, incident response, and data protection. While governance-oriented frameworks such as ISO/IEC 27001 and the NIST Cybersecurity Framework focus on organizational risk management and strategic oversight, PCI-DSS and NIST SP 800-53 emphasize operational and technical safeguards that support system security implementation [9], [11].

Despite their robustness, these frameworks often assume advanced technological infrastructure, continuous monitoring, and specialized cybersecurity expertise. Such requirements may be difficult to satisfy in digital microfinance institutions operating in low-resource environments. Consequently, the adoption of these frameworks within MFIs is often partial or symbolic, emphasizing documentation and regulatory compliance over fully operational security practices. Across the frameworks, a recurring weakness is inadequate accommodation of human and contextual vulnerabilities, especially in phishing [12].

These frameworks are conceptually sound but operationally incomplete when applied in MFI contexts, thereby prompting investigation of their adaptive performance in low-resource environments.

2.2. Application of Cybersecurity Frameworks in Microfinance Contexts

The adoption of frameworks within MFIs is partial and nominal. Severe budgetary, expertise, and infrastructural constraints limit implementation beyond policy documents [5], [11]. Most MFIs use cloud-based systems like NAMBUIT, which often have limited local expertise [13]. The requirements of frameworks, such as automated patching and continuous monitoring, are difficult to meet in rural or resource-limited environments [14].

Weak governance further undermines institutional resilience; most MFIs lack dedicated cybersecurity positions, robust audit controls, or regulatory oversight [15]. The behavioral dimension worsens these issues; phishing exploits psychological manipulation, linguistic trust, and social hierarchy [13], [16]. Field employees often fail to recognize phishing messages, which is a side effect of insufficient awareness training.

However, there are some localized adaptations. Some MFIs have used modular, low-cost practices, such as manual threat reporting, role-based access control, and peer simulation, which have shown quantifiable positive impacts [11]. These achievements show that modular, context-sensitive implementation can be effective in promoting resiliency despite resource limitations.

2.3. Phishing Threats in Digital Finance

The most widespread cyber threat in digital microfinance is phishing [17], [18]. It exploits system weaknesses and the cognitive and cultural patterns of trust in a low-income society. Manifestations included smishing, vishing, QR-code spoofing, and fake mobile applications. M-Pesa and Airtel Money services in East Africa are a particular focus for fraudsters, who use fraudulent alerts and impersonation messages [14], [19].

Behavioral vulnerabilities can enhance exposure, as users tend to trust community validation over technical verification [20]. Institutional reactions remain disjointed, as most organizations view phishing as a form of fraud and lack simulation drills or clear response guidelines [21]. The ensuing loss of trust poses a threat to financial inclusion [5] and underscores the need to align framework adoption with the effectiveness of phishing prevention measures.

2.4. Evaluating the Effectiveness of Frameworks

Empirical studies support the hypothesis that the frameworks strengthen governance systems; however, their effect on reducing phishing cases is not uniform. For example, Taherdoost [22] found ongoing phishing activity in ISO 27001-compliant Brazilian banks, whereas Dupont [10] found a lack of detection-focused interventions in Namibian institutions. The lack of key performance indicators for phishing, e.g., susceptibility rates or incident-reporting speed, prevents an accurate evaluation of organizational resilience [23]. By contrast, simulation-based interventions have shown a 27% decrease in vulnerability, regardless of the framework [9].

Modern research incorporates artificial intelligence into frameworks; GRU-based anomaly-detection networks improve phishing detection and response time [24]. However, implementing these solutions in microfinance institutions is hampered by technical and infrastructural limitations. As a result, traditional frameworks have underscored the importance of compliance, underscoring the need for hybrid socio-technical approaches.

2.5. Gaps in Existing Research

Although numerous studies have examined cybersecurity frameworks, most focus on commercial banks in developed economies [25], [26]. Very few studies analyze how these frameworks adapt to the realities of MFIs, characterized by low digital literacy, fragmented infrastructure, and limited budgets [27].

Theoretical foundations for human behavior are lacking: while phishing in MFIs exploits cognitive biases and social status, research continues to view human error as a minor factor [28]. Besides, AI-enhanced defense systems are rarely tested in low-resource environments [24]. Cross-sectional designs and audit-based scoring are methodological limitations that hinder understanding of framework performance over time [21].

To address these gaps, combined and comparative research evaluating contextual, behavioral, and technological aspects is required. This study responds directly by empirically assessing the efficacy of frameworks and by suggesting adaptive, AI-aided models for resource-constrained digital finance.

2.6. AI-Enhanced Phishing Detection in Low-Resource Settings

Recent developments in gated recurrent unit (GRU)-based neural networks offer promising, low-cost solutions for phishing detection in mobile finance environments. On-device inferences with TensorFlow Lite enable anomaly detection without high-bandwidth requirements. Prior studies report detection accuracies exceeding 90% and reductions in false-positive rates of more than 30% in both African and South Asian deployments [28], [29]. Integrating these adaptive models with traditional frameworks such as the NIST Cybersecurity Framework bridges the gap between policy compliance and operational resilience, thereby supporting scalable, context-aware defenses.

2.7. Theoretical Framework

This study adopts a socio-technical theoretical perspective integrating Protection Motivation Theory (PMT), the Design–Reality Gap model, and Resilience Engineering to explain how cybersecurity frameworks operate within digital microfinance institutions (MFIs).

Protection Motivation Theory provides an established behavioral framework for understanding how individuals respond to cybersecurity threats. PMT posits that protective behavior emerges through two cognitive processes: threat appraisal and coping appraisal. Threat appraisal evaluates the perceived severity and vulnerability of a threat, while coping appraisal assesses the efficacy of responses and self-efficacy. In organizational cybersecurity contexts, PMT has been widely applied to explain employee compliance with security policies and their ability to recognize phishing attacks. Employees who perceive phishing as a serious threat and believe they possess the skills to respond appropriately are more likely to report suspicious communications and follow security procedures. Conversely, insufficient training or punitive reporting environments reduce perceived self-efficacy and discourage proactive security behavior [1].

While PMT explains employee behavior at the individual level, institutional cybersecurity performance is also influenced by structural and technological factors. The Design–Reality Gap model provides a useful lens for understanding why externally developed cybersecurity frameworks may fail when implemented in resource-constrained environments. The model argues that information systems often fail when the design assumptions embedded within them do not align with the local institutional context in which they are implemented. In the case of MFIs,

many widely adopted cybersecurity frameworks assume the availability of dedicated security teams, centralized monitoring infrastructure, and continuous compliance auditing. These assumptions may not hold in smaller institutions with limited budgets, fragmented technological infrastructure, and evolving governance structures [3].

Resilience Engineering complements these perspectives by focusing on the adaptive capacity of socio-technical systems. Resilience-focused cybersecurity methods emphasize an organization's capacity to anticipate, identify, react to, and learn from disruptions, rather than strictly following predefined controls. In cybersecurity environments characterized by rapidly evolving threats, such as phishing, organizational resilience depends on the continuous interplay among technological defenses, governance mechanisms, and human behavior [3].

Integrating these three perspectives provides a comprehensive framework for evaluating the effectiveness of cybersecurity in digital MFIs. Protection Motivation Theory explains employee-level phishing detection behavior, the Design–Reality Gap model explains institutional challenges in implementing international cybersecurity frameworks, and Resilience Engineering highlights the importance of adaptive organizational practices. Together, these theories inform the conceptual foundation of the Adaptive Cybersecurity Framework proposed in this study, which integrates behavioral awareness, governance adaptation, and lightweight technological detection mechanisms to enhance institutional resilience against phishing attacks. Table 1 outlines how the theoretical foundations support the proposed Adaptive Cybersecurity Framework, showing how each perspective influences particular functional parts.

Table 1. Mapping of Theoretical Foundations to Framework Components

Theoretical Perspective	Framework Component	Functional Contribution
Protection Motivation Theory (PMT)	Behaviorally integrated security practices	Enhances user awareness, threat appraisal, and response efficacy
Design–Reality Gap Model	Modular governance structures	Enables alignment of cybersecurity controls with local institutional constraints
Resilience Engineering	Adaptive feedback and learning mechanisms	Supports continuous system adaptation, incident learning, and recovery

This mapping clarifies the interaction between behavioral, structural, and adaptive elements within the framework, thereby strengthening its conceptual coherence and analytical transparency.

3. METHODOLOGY

3.1. Research Design

A qualitative, dominant-mixed-methods, multiple-case study design was used in this research to assess the real-world effectiveness of internationally recommended cybersecurity frameworks, such as ISO/IEC 27001, the NIST Cybersecurity Framework (CSF), COBIT, and CIS Controls, in reducing phishing risks in digital microfinance institutions (MFIs) in low-resource environments. The qualitative part provided explanatory evidence of the behavioral and institutional processes affecting cybersecurity, and the quantitative element offered an opportunity to verify patterns and compare cases.

The sample consisted of six MFIs in Nairobi, intentionally selected to represent a wide range of regulatory, infrastructural, and cultural diversity. Regulated (Tier IV) and community-based (Tier III) MFIs were well represented in the study using a maximum-variation sampling model. The

mixed-methods approach enabled methodological triangulation, juxtaposing formal framework specifications with on-the-ground realities and clarifying the moderators of contextual phishing resilience through semi-structured interviews, document analysis, and surveys.

3.2. Sampling Strategy

The study targeted microfinance institutions (MFIs) that offer mobile or cloud-based financial services and have limited cybersecurity capabilities. Institutional selection followed a purposive sampling strategy based on three criteria: (a) the degree of digital integration within institutional operations; (b) documented exposure to phishing attacks or related cyber incidents; and (c) the presence of either formal or informal implementation of recognized cybersecurity frameworks. Nairobi provides a particularly relevant setting for this investigation due to its highly developed digital financial ecosystem and widespread use of mobile money platforms such as M-Pesa, which have expanded financial inclusion while simultaneously increasing exposure to phishing and other cyber-enabled fraud.

This study examined six digital MFIs that met the above criteria. Within these institutions, twenty-four key informants were interviewed, and 150 staff members participated in structured surveys. The respondent categories included IT officers, compliance managers, operational personnel, and field agents. These participant groups were selected to capture both technical and behavioral dimensions of cybersecurity practices, thereby enabling the study to examine how governance structures, employee awareness, and institutional processes collectively influence phishing detection and response within digital financial environments.

The selected sample size aligns with the principles of qualitative multiple-case study methodology, where the objective is analytical rather than statistical generalization. In multiple-case designs, cases are selected to enable theoretical replication, whereby each case contributes additional insights into the phenomenon under investigation. Contemporary methodological research suggests that samples ranging from 4 to 10 cases are generally sufficient to support cross-case comparison and theory development in complex organizational environments. The inclusion of six MFIs, therefore, provided an appropriate balance between analytical depth and comparative diversity, allowing a detailed examination of cybersecurity framework adoption, employee awareness, and phishing response practices across institutions operating within similar regulatory and technological contexts [1].

Access to participating institutions was facilitated through professional networks, including the Alliance for Financial Inclusion (AFI) and national microfinance associations. Participation was voluntary, and all respondents provided informed consent prior to data collection. Institutional anonymity and participant confidentiality were maintained throughout the research process in accordance with established research ethics guidelines and data protection standards.

3.3. Data Collection Methods

The data were collected using three supplementary tools: semi-structured interviews, institutional document review, and a structured staff survey.

Institutional experiences related to phishing, cybersecurity models, training, and incident response processes were investigated during the interviews. A unifying thematic guide ensured consistency in theme, classifying it along the dimensions of governance, detection, awareness, and response, thereby enabling comparability while allowing contextual flexibility. All interviews lasted 45-90 minutes, were recorded with permission, and transcribed verbatim.

The analysis of the documents was carried out systematically by reviewing cybersecurity policies, audit reports, awareness resources, and incident registers to assess the formalization of defense mechanisms and validate the interview results.

The surveys captured staff awareness, reporting behavior, and perceived effectiveness of the cybersecurity framework using Likert-scale and categorical items. The questionnaire was deemed clear and reliable, as verified by a pilot conducted on a randomly chosen MFI. Data collection was conducted from June to September 2025, and all instruments were aligned with the convergent mixed-methods guidelines promoted by Creswell and Plano-Clark [30].

3.4. Data Analysis

A convergent mixed-methods analytical methodology was used, combining qualitative and quantitative strands to provide a multidimensional understanding of framework performance.
A thematic analysis of the qualitative data was performed using NVivo version 14 from QSR International. Coding involved a combination of deductive categories based on the framework domains and inductive themes identified from participants' narratives. Themes were developed through repetitive case-to-case comparisons, facilitated by memoing and peer debriefing, to improve reliability and reflexivity.

Quantitative data analysis was performed with IBM SPSS Statistics version 28 (IBM Corp.). The descriptive statistics and chi-square tests examined the relationships among training exposure, awareness, and the frequency of phishing incidents. Qualitative insights were complemented by numerical patterns that were used to validate them.

The joint display matrix was used to integrate thematic patterns with statistical indicators that depict the joint influence of governance structures, behavioral factors, and contextual limitations on the development of phishing resilience. This convergence highlighted differences between adopting the nominal framework and developing actual defensive capability.

3.5. Ethical Considerations

The study followed the Belmont Report and the Declaration of Helsinki, receiving approval from the Institutional Review Board for its ethical considerations. Every organization and participant was anonymized using pseudonyms. Written or recorded verbal consent was taken beforehand. Ethical compliance also followed national data protection laws, such as the Kenya Data Protection Act of 2019. Positionality, ethical decisions, and interpretive neutrality were monitored reflexively through a researcher's journal, thereby ensuring integrity throughout the research.

This study received ethical approval from the National Commission for Science, Technology, and Innovation, with Approval License number NACOSTI/P/25/4176419. All procedures complied with relevant ethical standards for human subject research. Data collection, transcription, and initial analysis took place simultaneously from June to September 2025. This approach aligns with typical qualitative and mixed-methods research practices, where iterative analysis runs alongside data collection to develop themes and maintain methodological rigor.

4. RESULTS

4.1. Framework Adoption and Implementation Patterns

The adoption of frameworks across the six digital microfinance institutions (MFIs) remains fragmented and, in most cases, symbolic, due to infrastructural limitations and institutional mimicry. Only one institution achieved partial ISO/IEC 27001 certification, only its headquarters, leaving the decentralized mobile-agent network formally ungoverned. Some MFIs adapted the NIST Cybersecurity Framework controls selected to accommodate M-Pesa integration and transaction monitoring. In contrast, others relied on agent-based verification systems and informal oversight.

The policy templates included incomplete placeholders whose main purpose was to appear regulatory-compliant. One of the compliance officers commented, “The documents are present so that regulators can see them.” The MFIs' priorities differed: some focused on detecting fraud via SMS, while others focused on managing agent credentials. At the same time, some lacked dedicated cybersecurity staff or formal escalation channels. Phishing-specific components, such as training simulations, awareness modules, and behavioral metrics, were absent from all institutions.

These findings illustrate the Design-Reality Gap described by Masiero [31], in which frameworks designed for high-resource environments fail to account for the sociotechnical constraints of MFIs. Subsequently, implementation has remained policy-based rather than behaviorally embedded, thereby limiting practical defensive capabilities despite increased documentation compliance. The partial operationalization directly shapes the pattern of phishing exposure, as discussed in the next section.

To improve clarity in cross-case analysis, Table 2 highlights key features of the six microfinance institutions, such as framework adoption, phishing exposure, detection capabilities, and training methods.

Table 2. Cross-Case Comparison of Participating MFIs

MFI	Framework Adoption	Phishing Incident Trend	Detection Time	Training Provision	Local Adaptation
MFI-01	Partial ISO 27001	Increasing	>48 hours	None	Compliance-focused documentation
MFI-02	Adapted NIST CSF	Moderate	24–48 hours	Limited	Informal peer reporting
MFI-03	Minimal framework use	High	>48 hours	None	No structured adaptation
MFI-04	Localized NIST CSF	Decreasing	<24 hours	Present	Simulation exercises and localized alerts
MFI-05	Mixed framework elements	Moderate	24–48 hours	Limited	Role-based access control
MFI-06	Minimal framework use	High	>48 hours	None	Informal communication channels

The comparison highlights substantial variation in implementation practices and outcomes across institutions, reinforcing the finding that contextual adaptation and behavioral integration play a critical role in enhancing phishing resilience beyond the adoption of formal frameworks.

4.2. Phishing Incident Patterns

The phishing incidents, which were common and varied over the past 18 months, were systematically underreported across all MFIs. The attacks targeted mobile service channels, agent communications, and administrative email accounts, using vectors such as SMS-based credential harvesting, internal email impersonation, and WhatsApp group spoofing. Two institutions reported voice-phishing (vishing) incidents in which attackers used local dialects to impersonate regulators, suggesting a prior data compromise.

There was no consistency in reporting mechanisms: only one MFI had a centralized log, while others relied on informal communication. One of the supervisors remarked, “You realize that you have lost money after losing it.” This was supported by survey data: only 28% of staff members had received specific training on phishing; 47% did not correctly identify simulated phishing messages; and 60% said they would report the incident to a coworker rather than to IT personnel.

These results show that there is a disproportionate security incentive system [32], [33], in which formal detection systems are perceived to cost more than the anticipated benefits, thereby sustaining chronic underinvestment. There was limited learning from incidents, as no institution updated its training or policies after the attacks. Based on this, phishing evolved into a normalized operational practice, condoned by weak detection capabilities and a lack of feedback loops.

4.3. Staff Awareness and Behavioral Dynamics

The main weakness that was shared across the institutions was human behavior. The level of phishing awareness was low despite the presence of the IT policies, especially among frontline and non-technical staff. Only 28% of employees received specific phishing training, and it was provided only once at induction. One of the loan officers at MFI-06 remarked, “We were advised to be wary, but nobody showed what a phishing message looks like.”

These gaps were validated through survey-based behavioral assessments; almost half of the respondents misclassified phishing incidents, and a majority preferred informal peer escalation over formal reporting. To illustrate these behavioral vulnerabilities more clearly, Table 3 summarizes key survey indicators on phishing awareness, detection ability, and incident reporting behavior among staff members across participating MFIs.

Table 3. Staff Phishing Awareness, Detection Accuracy, and Reporting Behavior

Indicator	Observed Result
Staff receiving formal phishing awareness training	28%
Staff correctly identifying simulated phishing messages	53%
Staff misclassifying phishing attempts	47%
Staff preferring informal peer reporting over IT escalation	60%
Institutions conducting simulated phishing exercises	0%

Note: Results based on structured survey responses from 150 employees across six participating MFIs. Percentages reflect aggregated responses from frontline staff, operational personnel, compliance officers, and IT staff.

The findings highlight the central role of behavioral factors in phishing vulnerability, reinforcing the importance of awareness training and supportive reporting environments.

The distribution of phishing awareness indicators among surveyed staff is further illustrated in Figure 1, which compares training exposure, phishing detection accuracy, and reporting behavior across participating institutions.

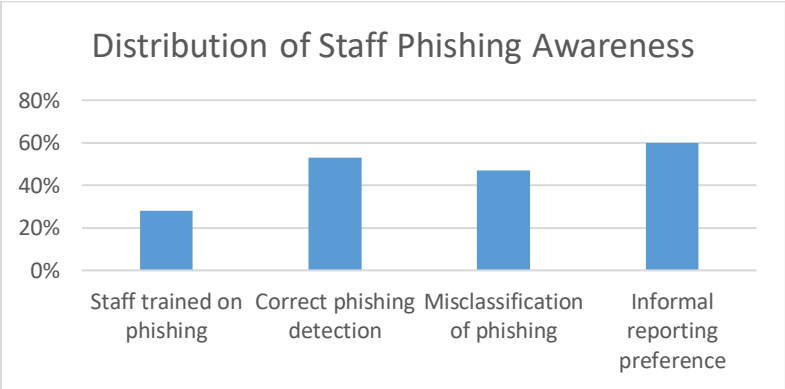

Figure 1. Distribution of Staff Phishing Awareness and Detection Indicators

Note: Percentages are derived from aggregated responses of 150 employees across six participating MFIs, including IT personnel, operational staff, compliance officers, and field agents.

The figure illustrates key behavioral findings from the staff survey conducted across six participating microfinance institutions. The results indicate limited exposure to phishing training and high misclassification rates, with most staff preferring informal reporting channels over formal IT escalation procedures.

Role awareness also differed significantly: IT personnel were more confident, while agents and call center employees were more uncertain. None of the MFIs performed simulated phishing tests, reflecting weak learning cultures.

Interviews also revealed punitive responses; two staff members cited disciplinary measures after phishing incidents, therefore, promoting silence and underreporting. This pattern aligns with Bada and Sasse [34] and Nurse et al. [35], who argue that blame-centric environments erode transparency and hinder organizational learning. According to the Protection Motivation Theory (PMT), variables such as inconsistent training and punitive feedback reduce self-efficacy and threat appraisal [31], [36]. Thus, compliance behavior remains reactive, and institutions' resilience depends on fostering psychological safety and continuous, supportive learning.

4.4. Framework Effectiveness and Performance Metrics

Triangulated data from interviews, surveys, and institutional documents reveal a significant discrepancy between policy formulation and operational outcomes. Each surveyed microfinance institution (MFI) mentioned at least one global framework, and only two reported empirically

measurable reductions in phishing. Phishing reduction measures the percentage change in reported phishing incidents over a year within participating institutions, using data from logs and staff reports. Detection performance is assessed through mean time to detect (MTTD) and mean time to respond (MTTR), based on incident logs and response records.

When metrics were available (MFI-02), the mean time to detect (MTTD) ranged from 18 to 36 hours, while the mean time to respond (MTTR) ranged from 24 to 48 hours. Often, detection occurred after client complaints rather than through proactive monitoring. In other institutions, delays exceeded 48 hours, highlighting a lack of real-time detection capacity.

A chi-square test of independence was conducted to examine the association between phishing awareness training and the ability to correctly detect phishing attempts ($\chi^2 = 6.84$, df = 1, $p = 0.009$, N = 150). The findings reveal a statistically significant relationship, indicating that staff who underwent phishing awareness training are more likely than those without it to identify phishing attempts correctly. Nonetheless, because the study primarily uses a qualitative-dominant mixed-methods approach, these statistical results are viewed as supportive rather than conclusive and serve to enhance the qualitative insights gathered from interviews and institutional data.

The comparative trend analysis showed that MFI-04, which localized NIST CSF controls through simulation exercises and simplified agent reporting, reduced phishing by 35% over one year. However, MFI-01, where ISO 27001 documentation was maintained without reinforcing behavior, saw a 22% increase in incidents. Controls associated with phishing averaged 0.8/3, while general policy domains, such as access control, averaged 2.1/3. Statistically, there was no notable difference in phishing vulnerability between framework-adopting and non-adopting institutions (Click-through rates = 46% vs 49%). These click-through rates are based on aggregated staff survey responses rather than controlled phishing simulations. Consequently, they should be viewed as approximate indicators of user susceptibility rather than exact behavioral data collected under experimental conditions. This pattern aligns with street-level bureaucracy theory [37], [38]. This suggests that employees adapt to or circumvent procedures to meet situational demands.

Institutions that localized frameworks by adding local-language alerts, SMS-based reporting, and modular response protocols reported a 30-42% improvement in response efficiency despite minimal formal certification. These positive empirical results support the Design-Reality Gap Model by Masiero [31] and illustrate that adaptive, modular implementation creates stronger phishing resilience than strict compliance.

In conclusion, adopting the framework increases visibility into compliance but rarely translates into defensive capacity. Institutional resilience develops where frameworks are contextually responsive, behaviorally enforced, and operationally modular, principles that form the basis of the Adaptive Cybersecurity Framework described in the next section.

5. DISCUSSION

5.1. Interpretation of Findings

The results indicate that, despite increasing references to international cybersecurity standards in digital microfinance institutions (MFIs), their protection against phishing remains symbolic and fragmented. Adoption of policies has outpaced the development of behavioral and procedural preparedness, resulting in a persistent gap between documented compliance and operational

resilience. The problem of phishing is rampant but systematically underreported, creating an awareness-action gap.

Institutional culture and human behavior have a greater impact on phishing resilience than the presence of cybersecurity frameworks. The staff demonstrated limited ability to detect phishing attempts and relied on informal escalation methods. The lack of organized training or simulation led to reactive rather than preventive responses. As a result, frameworks without behavioral reinforcement produced only superficial preparedness, a tendency akin to prior studies on the behavioral boundaries of compliance-based cybersecurity [36], [39]. These observations provide a foundation for understanding why formal frameworks fail to become practical resilience.

5.2. Gaps in Frameworks and Contextual Limitations

One of the main findings from this research concerns the discrepancy between international cybersecurity models and the operational realities of MFIs. Standards such as ISO/IEC 27001 and the NIST CSF assume stable infrastructure, dedicated security staff, and continuous monitoring, conditions rarely found in low-bandwidth, resource-constrained environments where IT functions are typically part-time or outsourced. MFI-03 and MFI-06 are examples of this structural infeasibility, demonstrating real-time detection despite the adoption of nominal frameworks.

This inconsistency is an example of the Design-Reality Gap, as described by Masiero [31], in which externally engineered systems do not work within the contextual constraints. In addition, a significant number of MFIs take part in isomorphic mimicry [40]. Frameworks are adopted for donor or regulatory legitimacy rather than for practical defense. The current standards are insufficient to address phishing-specific vulnerabilities rooted in linguistic knowledge, informal communication, and socio-cultural trust. The outcome is a policy architecture that is not optimal in the socially engineered attacks that predominate in digital financial ecosystems.

5.3. Human Factors and Organizational Readiness

Human behavior and psychology have a greater impact on organizational resilience than documentation does. Only 28% percent of the employees reported being trained on phishing, and the vast majority relied on informal means of reporting. This reactive stance exemplifies the concept of normalization of deviance, as described by Bada & Sasse [34] and Alraja et al. [39], in which repeated exposure to the risk without correction normalizes vulnerability.

Through the lens of Protection Motivation Theory (PMT), when perceived efficacy is low and institutional support is weak, employees are inclined to underestimate threats or shift responsibility [36]. Punitive reactions observed in MFI-01 and MFI-02, where the staff was reprimanded after incidents, sabotaged the self-efficacy and discouraged disclosure, consistent with Bada & Sasse [34] and Nurse et al. [35]. The only way reform can be effective is by shifting from a culture of compliance rhetoric to learning cultures that are psychologically safe and treat errors as opportunities for feedback—incorporating phishing awareness into daily operations and using non-punitive reinforcement—shifting defense toward adaptive vigilance rather than rule-following.

5.4. Comparative and Regional Perspective

The research shows a significant difference in the ability of MFIs and institutions in developed countries to respond to phishing. However, financial organizations based in OECD countries have a mean response time of less than six hours [41]. The MFIs discussed in this paper had a mean response time of 24-48 hours, typically responding after the incident. Weak regulatory

oversight across Tier III and Tier IV MFIs worsens the situation by reducing incentives for proactive investment.

However, local innovations indicate latent adaptive ability. Phishing warnings embedded in WhatsApp bulletins (MFI-04) or peer-to-peer shortcuts to escalation (MFI-02), among other practices, improved detection, even though they were not formally structured. These informal adaptations display resilience potential, which is often overlooked by standardized frameworks. Nevertheless, such practices remain susceptible to turnover and discontinuity unless they are institutionalized. It is now important to formalize and scale these grassroots innovations into the governance systems, a transition explored through the adaptive framework proposed below.

The findings provide a clear, integrated response to the research questions. Phishing patterns (Research Question 1) mostly involve SMS, email impersonation, and social engineering tactics (Section 4.2). Regarding framework effectiveness (Research Question 2), the results show that relying solely on compliance-based adoption does not reduce vulnerability, with similar click-through rates (46% versus 49%) and inconsistent incident outcomes (Section 4.4). Behavioral and governance issues (Research Question 3) highlight gaps in awareness, reporting, and institutional enforcement (Section 4.3). Finally, adaptive mechanisms (Research Question 4) are demonstrated by improved results in localized implementations, which underpin the proposed framework (Section 5.5).

5.5. An Adaptive Cybersecurity Framework for Resource-Constrained Financial Ecosystems

Building on the findings of this study, an Adaptive Cybersecurity Framework for Resource-Constrained Financial Ecosystems is proposed to address limitations of conventional cybersecurity frameworks in digital microfinance institutions (MFIs). The framework reconciles international standards with local operational realities by integrating three mutually reinforcing pillars: AI-assisted threat intelligence, modular governance structures, and behaviorally integrated security practices.

The first pillar involves AI-assisted threat intelligence, implemented with lightweight machine-learning techniques that identify phishing patterns across communication channels commonly used in digital finance ecosystems. In this framework, Gated Recurrent Units (GRUs) are proposed as a conceptual detection mechanism due to their relatively low computational complexity compared with other recurrent neural networks. Prior research shows that GRU-based models achieve high phishing-detection accuracy while requiring fewer parameters and reducing training time, making them suitable for bandwidth-constrained environments [28]. When combined with federated learning approaches, MFIs could collaboratively improve detection models while maintaining institutional data sovereignty [27].

The second pillar focuses on modular governance structures that translate high-level cybersecurity frameworks into simplified operational controls for resource-constrained institutions. Instead of a rigid, compliance-oriented implementation, governance mechanisms are adapted to local contexts through tiered incident-reporting systems, such as SMS-based reporting for smaller institutions and USSD-based escalation for larger networks. This modular approach enables institutions to transform cybersecurity frameworks from static compliance instruments into practical operational tools that support real-time incident response. Such flexibility reflects the growing recognition that frontline actors often adapt policy implementation to fit organizational realities [37], [38].

The third pillar emphasizes behaviorally integrated security practices, which address the human factors underlying phishing vulnerability. Contextual phishing awareness training, localized communication strategies, and non-punitive reporting mechanisms help strengthen employee self-efficacy and improve incident reporting. These practices align with Protection Motivation Theory, which highlights the importance of threat perception and response efficacy in motivating protective cybersecurity behavior [36].

Together, these three components create a continuous adaptive cycle in which technological detection mechanisms identify emerging threats, governance structures coordinate institutional responses, and behavioral practices reinforce organizational vigilance. This interaction reflects the principles of resilience engineering, which emphasize the capacity of socio-technical systems to anticipate, respond to, and learn from disruptions [42]. The operational interaction between the three pillars and the resulting adaptive learning cycle is illustrated in Figure 2. The framework depicts how phishing threats enter the digital financial ecosystem and are processed through successive layers of technological detection, governance coordination, and human behavioral response. Incident outcomes then feed back into organizational learning processes, improving detection models, governance procedures, and staff awareness programs over time.

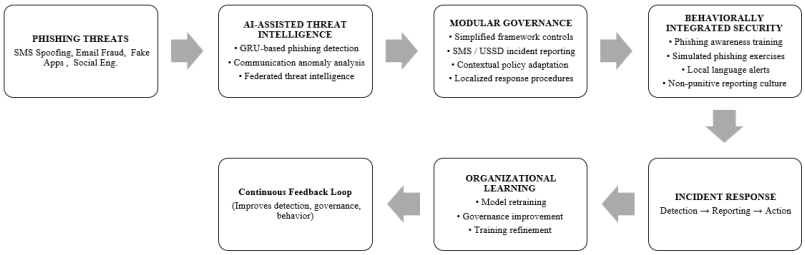

Figure 2. Adaptive Cybersecurity Framework for Resource-Constrained Financial Ecosystems.

The framework illustrates the interaction among AI-assisted threat intelligence, modular governance structures, and behaviorally integrated security practices to strengthen phishing resilience within digital microfinance institutions. Phishing threats entering institutional communication channels are processed through successive technological, organizational, and behavioral layers that support detection, reporting, and response. Incident outcomes generate a continuous feedback loop that improves detection models, governance procedures, and employee awareness, thereby enabling adaptive cybersecurity resilience in resource-constrained financial environments. By integrating technological feasibility, institutional flexibility, and human behavior, the proposed framework positions cybersecurity as a core organizational capability rather than a peripheral compliance requirement.

Traditional frameworks like ISO/IEC 27001 and NIST CSF focus on compliance and standardized controls, which might be less effective if not adapted to specific contexts, especially in resource-limited settings. This is supported by findings showing that compliance-focused approaches (such as MFI-01) led to a 22% increase in phishing attacks. In contrast, adaptive strategies (such as MFI-04) resulted in a 35% decrease and faster detection times (<24 hours). Conversely, the proposed Adaptive Cybersecurity Framework combines behavioral reinforcement, modular governance, and lightweight AI-driven detection to support cybersecurity management that is tailored to the environment and operational needs.

The detection component of the proposed framework, based on a GRU, draws on prior research demonstrating the effectiveness of lightweight deep learning models for phishing detection. However, it was neither implemented nor empirically tested within the microfinance institutions

involved in this study. Therefore, the Adaptive Cybersecurity Framework should be seen as an empirically informed and theoretically supported design proposal, not a fully validated technical solution.

Future research ought to concentrate on pilot testing and methodical performance assessment of the GRU-based system in resource-limited financial settings to evaluate its practical viability and efficiency.

5.6. Limitations

This study focuses on six digital microfinance institutions located within Nairobi, Kenya. It therefore reflects a context-specific analysis shaped by the regulatory, infrastructural, and socio-economic conditions of this setting. While the multiple-case study design supports analytical generalization, the findings should not be interpreted as statistically generalizable to all microfinance institutions or to other geographic regions.

In addition, phishing incidents were frequently underreported across participating institutions, as evidenced by the reliance on informal reporting methods and the absence of a centralized logging system. This limitation may affect the completeness of incident-based data, suggesting that actual phishing exposure may be higher than reported.

Furthermore, the study did not employ controlled phishing simulations. As a result, behavioral measures such as detection accuracy and response tendencies are derived primarily from self-reported survey data and retrospective accounts, which may be subject to recall bias or social desirability effects.

6. CONCLUSION

As this discussion shows, cybersecurity success in microfinance institutions (MFIs) depends on contextual factors, behavioral mediation, and adaptive design. Conventional frameworks meet documentation requirements but rarely achieve operational resilience. The current study redefines cybersecurity as an emerging socio-technical system by incorporating Protection Motivation Theory, Design-Reality Gap Theory, and Resilience Engineering.

This study contributes to cybersecurity governance research in three ways. Firstly, it offers one of the few empirical assessments of the effectiveness of cybersecurity frameworks for digital microfinance institutions operating in resource-limited settings. Second, it integrates the behavioral, governance, and technological dimensions within a socio-technical analytical framework to understand phishing resilience in digital finance ecosystems. Third, it proposes an adaptive cybersecurity architecture that combines lightweight, AI-assisted detection mechanisms with modular governance and behaviorally integrated security practices, offering a practical pathway to strengthen phishing resilience in low-resource financial systems.

Theoretically, this integration explains the evolution of adaptive modularity and behavioral embedding, which convert static frameworks into a dynamic ecosystem that learns and responds continuously. In practice, the consequent suggestion provides a roadmap for strategic direction for regulators, donors, and financial networks seeking to introduce scalable, contextually appropriate cybersecurity reform.

Policy-wise, implementing adaptive governance and federated AI architectures offers an opportunity to improve collective defense across microfinance ecosystems. Future research

should conduct longitudinal evaluations of the proposed framework to determine the impact of ongoing learning cycles on institutional trust and systemic resilience in digital finance.

Future research should extend this work by adopting a longitudinal study design to evaluate the real-world implementation of the proposed Adaptive Cybersecurity Framework over time. Such research should include pilot deployments within selected microfinance institutions to assess operational feasibility, scalability, and contextual adaptability in resource-constrained environments. Key evaluation metrics should include phishing detection accuracy, mean time to detect (MTTD), mean time to respond (MTTR), user awareness improvement, and incident reporting rates. In addition, future studies should investigate the integration and performance of the proposed GRU-based detection mechanism within live institutional systems to determine its effectiveness under real-world operational conditions.

ACKNOWLEDGEMENT

The authors appreciate the participating Microfinance Institutions and respondents for their cooperation and openness during data collection. The authors declare no conflicts of interest.

REFERENCES

[1] S. Wang, M. Asif, M. F. Shahzad, and M. Ashfaq, "Data privacy and cybersecurity challenges in the digital transformation of the banking sector," Computers & Security, vol. 147, p. 104051, Dec. 2024, doi: 10.1016/j.cose.2024.104051.

[2] "INTERPOL Financial Fraud assessment: A global threat boosted by technology." Accessed: Feb. 26, 2026. [Online]. Available: https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-Financial-Fraud-assessment-A-global-threat-boosted-by-technology

[3] L. Ribeiro, I. S. Guedes, and C. S. Cardoso, "Which factors predict susceptibility to phishing? An empirical study," Computers & Security, vol. 136, p. 103558, Jan. 2024, doi: 10.1016/j.cose.2023.103558.

[4] A. Zimba, K. Phiri, C. Kashale, and M. Phiri, "Unveiling deception: a socio-economic analysis of smishing attacks on mobile money transaction users," Humanit Soc Sci Commun, vol. 12, no. 1, p. 1880, Dec. 2025, doi: 10.1057/s41599-025-06141-8.

[5] D. Susie Lesley Sarah, Lonie, "Digital financial services and risk management : handbook," World Bank. Accessed: Feb. 26, 2026. [Online]. Available: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/226461531293264583

[6] "Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach | MDPI." Accessed: Feb. 25, 2026. [Online]. Available: https://www.mdpi.com/2079-9292/12/17/3629

[7] Y. Harel and A. Carmeli, "A strategic cybersecurity oversight framework: a board's imperative," J Cyber Secur, vol. 11, no. 1, p. tyaf021, Jan. 2025, doi: 10.1093/cybsec/tyaf021.

[8] J. L. Salas-Riega, Y. Riega-Virú, M. Ninaquispe-Soto, and J. M. Salas-Riega, "Cybersecurity and the NIST Framework: A Systematic Review of its Implementation and Effectiveness Against Cyber Threats," International Journal of Advanced Computer Science and Applications (ijacsa), vol. 16, no. 6, Jun. 2025, doi: 10.14569/IJACSA.2025.0160672.

[9] J. Prümmer, T. van Steen, and B. van den Berg, "A systematic review of current cybersecurity training methods," Computers & Security, vol. 136, p. 103585, Jan. 2024, doi: 10.1016/j.cose.2023.103585.

[10] B. Dupont, "The cyber-resilience of financial institutions: significance and applicability," J Cyber Secur, vol. 5, no. 1, p. tyz013, Jan. 2019, doi: 10.1093/cybsec/tyz013.

[11] Y. T. Y. Azura, M. A. Azad, and Y. Ahmed, "An integrated cyber security risk management framework for online banking systems," J BANK FINANC TECHNOL, vol. 9, no. 1, pp. 85–104, Apr. 2025, doi: 10.1007/s42786-025-00056-3.

[12] K. Khadka and A. B. Ullah, "Human factors in cybersecurity: an interdisciplinary review and framework proposal," Int. J. Inf. Secur., vol. 24, no. 3, p. 119, Apr. 2025, doi: 10.1007/s10207-025-01032-0.
[13] N. Kshetri, "Cybercrime and Cybersecurity in Africa," Journal of Global Information Technology Management, vol. 22, no. 2, pp. 77–81, Apr. 2019, doi: 10.1080/1097198X.2019.1603527.
[14] "Cybersecurity for financial inclusion: framework & risk guide," Alliance for Financial Inclusion, Kuala Lumpur, Malaysia, 2019. Accessed: Jan. 05, 2026. [Online]. Available: https://www.afi-global.org/publication/cybersecurity-for-financial-inclusion-framework-risk-guide/
[15] "Open Knowledge Repository." Accessed: Mar. 01, 2026. [Online]. Available: https://openknowledge.worldbank.org/entities/publication/f3add773-227f-58f4-a818-548ec471919d
[16] "Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity | ENISA." Accessed: Feb. 25, 2026. [Online]. Available: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity
[17] "Suspicion, Cognition, and Automaticity Model of Phishing Susceptibility - Arun Vishwanath, Brynne Harrison, Yu Jie Ng, 2018." Accessed: Feb. 26, 2026. [Online]. Available: https://journals.sagepub.com/doi/10.1177/0093650215627483
[18] M. Waliullah, M. Z. H. George, M. T. Hasan, M. K. Alam, M. S. K. Munira, and N. A. Siddiqui, "Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: a systematic literature review," AJATES, vol. 1, no. 01, pp. 226–257, Feb. 2025, doi: 10.63125/fh49gz18.
[19] "Responsible Digital Credit: Frontier Solutions for Authorities and Providers." Accessed: Feb. 25, 2026. [Online]. Available: https://www.cgap.org/research/publication/responsible-digital-credit-frontier-solutions-for-authorities-and-providers?utm_source=chatgpt.com
[20] M. Butavicius, R. Taib, and S. J. Han, "Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of phishing emails," Computers & Security, vol. 123, p. 102937, Dec. 2022, doi: 10.1016/j.cose.2022.102937.
[21] P. Alaeifar, S. Pal, Z. Jadidi, M. Hussain, and E. Foo, "Current approaches and future directions for Cyber Threat Intelligence sharing: A survey," Journal of Information Security and Applications, vol. 83, p. 103786, Jun. 2024, doi: 10.1016/j.jisa.2024.103786.
[22] H. Taherdoost, "Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview," Electronics, vol. 11, no. 14, Jul. 2022, doi: 10.3390/electronics11142181.
[23] D. A. Sepúlveda Estay, R. Sahay, M. B. Barfod, and C. D. Jensen, "A systematic review of cyber-resilience assessment frameworks," Computers & Security, vol. 97, p. 101996, Oct. 2020, doi: 10.1016/j.cose.2020.101996.
[24] Q. E. ul Haq, M. H. Faheem, and I. Ahmad, "Detecting Phishing URLs Based on a Deep Learning Approach to Prevent Cyber-Attacks," Applied Sciences, vol. 14, no. 22, Nov. 2024, doi: 10.3390/app142210086.
[25] D. Javaheri, M. Fahmideh, H. Chizari, P. Lalbakhsh, and J. Hur, "Cybersecurity threats in FinTech: A systematic review," Expert Systems with Applications, vol. 241, p. 122697, May 2024, doi: 10.1016/j.eswa.2023.122697.
[26] N. N. Cele and S. Kwenda, "Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review," Journal of Financial Crime, vol. 32, no. 1, pp. 31–48, Apr. 2024, doi: 10.1108/JFC-10-2023-0263.
[27] S. Cheng, J. Li, L. Luo, and Y. Zhu, "Cybersecurity governance and digital finance: Evidence from sovereign states," Finance Research Letters, vol. 65, p. 105533, Jul. 2024, doi: 10.1016/j.frl.2024.105533.
[28] M. Penmetsa, J. R. Bhumireddy, R. Chalasani, S. R. Vangala, R. M. Polam, and B. Kamarthapu, "Effectiveness of Deep Learning Algorithms in Phishing Attack Detection for Cybersecurity Frameworks," Journal of Data Analysis and Information Processing, vol. 13, no. 3, pp. 331–346, Aug. 2025, doi: 10.4236/jdaip.2025.133021.
[29] Z. Alshingiti, R. Alaqel, J. Al-Muhtadi, Q. E. U. Haq, K. Saleem, and M. H. Faheem, "A Deep Learning-Based Phishing Detection System Using CNN, LSTM, and LSTM-CNN," Electronics, vol. 12, no. 1, Jan. 2023, doi: 10.3390/electronics12010232.
[30] "Designing and Conducting Mixed Methods Research," SAGE Publications Ltd. Accessed: Feb. 25, 2026. [Online]. Available: https://uk.sagepub.com/en-gb/eur/designing-and-conducting-mixed-methods-research/book269004

[31] S. Masiero, "The Origins of Failure: Seeking the Causes of Design–Reality Gaps," Information Technology for Development, vol. 22, no. 3, pp. 487–502, Jul. 2016, doi: 10.1080/02681102.2016.1143346.
[32] T. Moore, "The economics of cybersecurity: Principles and policy options," International Journal of Critical Infrastructure Protection, vol. 3, no. 3, pp. 103–117, Dec. 2010, doi: 10.1016/j.ijcip.2010.10.002.
[33] J. Park, D. Cho, J. K. Lee, and B. Lee, "The Economics of Cybercrime: The Role of Broadband and Socioeconomic Status," ACM Trans. Manage. Inf. Syst., vol. 10, no. 4, p. 13:1-13:23, Dec. 2019, doi: 10.1145/3351159.
[34] M. Bada, A. M. Sasse, and J. R. C. Nurse, "Cyber Security Awareness Campaigns: Why do they fail to change behaviour?," Jan. 09, 2019, arXiv: arXiv:1901.02672. doi: 10.48550/arXiv.1901.02672.
[35] J. R. C. Nurse, S. Creese, M. Goldsmith, and K. Lamberts, "Guidelines for usable cybersecurity: Past and present," in 2011 Third International Workshop on Cyberspace Safety and Security (CSS), Sep. 2011, pp. 21–26. doi: 10.1109/CSS.2011.6058566.
[36] T. Herath and H. R. Rao, "Protection motivation and deterrence: a framework for security policy compliance in organisations," European Journal of Information Systems, vol. 18, no. 2, pp. 106–125, Apr. 2009, doi: 10.1057/ejis.2009.6.
[37] A. Chang and Gene. A. Brewer, "Street-Level bureaucracy in public administration: A systematic literature review," Public Management Review, vol. 25, no. 11, pp. 2191–2211, Nov. 2023, doi: 10.1080/14719037.2022.2065517.
[38] P. Rossi, S. Tuurnas, and J. Stenvall, "Street-level bureaucrats as policymakers in the implementation of information system in social services," Public Management Review, vol. 27, no. 3, pp. 702–721, Mar. 2025, doi: 10.1080/14719037.2024.2362247.
[39] M. N. Alraja, U. J. Butt, and M. Abbod, "Information security policies compliance in a global setting: An employee's perspective," Computers & Security, vol. 129, p. 103208, Jun. 2023, doi: 10.1016/j.cose.2023.103208.
[40] L. Pritchett, M. Woolcock, and M. Andrews, "Looking Like a State: Techniques of Persistent Failure in State Capability for Implementation," The Journal of Development Studies, vol. 49, no. 1, pp. 1–18, Jan. 2013, doi: 10.1080/00220388.2012.709614.
[41] "2025 Data Breach Investigations Report," Verizon Business. Accessed: Mar. 01, 2026. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/
[42] D. D. Woods, "Four concepts for resilience and the implications for the future of resilience engineering," Reliability Engineering & System Safety, vol. 141, pp. 5–9, Sep. 2015, doi: 10.1016/j.ress.2015.03.018.

AUTHORS

Richard Mathenge is a lecturer, researcher, and Ph.D. candidate in Information Technology at Kirinyaga University. His research interests include machine learning and cybersecurity.

Dr. Catherine Wambui Mukunga is a lecturer at Kirinyaga University, Kenya. She received her M.Sc. in Computer Science in 2014 from the University of Nairobi, Kenya, and her B.Sc. in Information Technology in 2009 from Jomo Kenyatta University of Agriculture and Technology, Kenya. She holds a Doctor of Philosophy in Information Technology degree from Murang'a University of Technology, Kenya, in 2023. She started her career in University teaching at the Technical University of Kenya in September 2015. Her research activities are related to Software Engineering Metrics, Software Project Management, Network Security and Machine Learning. She can be contacted at cmukunga@kyu.ac.ke.

Dr. Ephantus Mwangi is a scholar in Information Technology with a Ph.D. from Murang'a University, Kenya. He holds an M.Sc. in Information Systems from Kisii University and a Bachelor of Education in Science (Mathematics and Computer Science) from Kabarak University. His research interests span network security, data science, data analytics, machine learning, and cloud computing.