Scientific Research Publishing

Journal of Information Security, 2025, 16(1), 114-130
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

A Review of Human Vulnerabilities in Cyber Security: Challenges and Solutions for Microfinance Institutions

Evaline Waweru[1], Simon Maina Karume[2], Alex Kibet[3]

[1]Department of Computing and Informatics, The Cooperative University, Nairobi, Kenya
[2]Department of Computer Science and Information Technology, Kabarak University, Nakuru, Kenya
[3]Department of Computing and Informatics, Laikipia University, Laikipia, Kenya
Email: ewaweru@cuk.ac.ke, skarume@cuk.ac.ke, akibet@laikipia.ac.ke

How to cite this paper: Waweru, E., Karume, S.M. and Kibet, A. (2025) A Review of Human Vulnerabilities in Cyber Security: Challenges and Solutions for Microfinance Institutions. *Journal of Information Security*, **16**, 114-130.
https://doi.org/10.4236/jis.2025.161006

Received: November 5, 2024
Accepted: December 28, 2024
Published: December 31, 2024

Abstract

This review examines human vulnerabilities in cybersecurity within Microfinance Institutions, analyzing their impact on organizational resilience. Focusing on social engineering, inadequate security training, and weak internal protocols, the study identifies key vulnerabilities exacerbating cyber threats to MFIs. A literature review using databases like IEEE Xplore and Google Scholar focused on studies from 2019 to 2023 addressing human factors in cybersecurity specific to MFIs. Analysis of 57 studies reveals that phishing and insider threats are predominant, with a 20% annual increase in phishing attempts. Employee susceptibility to these attacks is heightened by insufficient training, with entry-level employees showing the highest vulnerability rates. Further, only 35% of MFIs offer regular cybersecurity training, significantly impacting incident reduction. This paper recommends enhanced training frequency, robust internal controls, and a cybersecurity-aware culture to mitigate human-induced cyber risks in MFIs.

Keywords

Human Vulnerabilities, Cybersecurity, Microfinance Institutions, Cyber Threats, Cybersecurity Awareness, Risk Mitigation

1. Introduction

1.1. Background Study

Microfinance Institutions (MFIs) are essential in advancing financial inclusion, especially in developing nations [1]. They offer financial services to marginalized

communities, allowing them to obtain credit, savings, and insurance options. Nevertheless, with the growing use of digital technologies by MFIs to improve service delivery, they are at a higher risk of cyber threats [2] [3].

The cyber security environment for MFIs is intricate, marked by an increasing frequency of cyber-attacks that take advantage of human weaknesses like social engineering and insider risks [4]. MFIs, along with other parts of the financial industry, are a main focus for cybercriminals because of the sensitive information they manage and the potential profits from successful breaches [5].

The cyber security landscape for MFIs is characterized by a unique set of challenges that stem from their operational frameworks [4] and the socio-economic contexts [2] in which they operate. According to [4], MFIs often lack the financial resources to invest in advanced cyber security measures, making them susceptible to attacks such as data breaches and financial fraud [6] [7].

Furthermore, [4] indicates that limited awareness of cyber security protocols among employees exacerbates these vulnerabilities, as staff members may not recognize the importance of adhering to security practices [8]. The increasing sophistication of cyber threats, like social engineering attacks [9], poses significant risks to the integrity and confidentiality of sensitive financial data held by MFIs [10] [11]. Human vulnerabilities are often cited as the weakest link in cyber security frameworks [12].

Employees may inadvertently compromise security through negligence or lack of awareness, making it imperative for MFIs to address these vulnerabilities [13]. Research indicates that enhancing employee awareness and knowledge about cyber security can significantly mitigate risks associated with human error [14]. Additionally, organizational culture within MFIs can either exacerbate or alleviate these vulnerabilities, highlighting the need for a comprehensive approach to cyber security that includes training and awareness programs.

1.2. Statement of the Problem

Although microfinance institutions (MFIs) play a crucial part in enhancing financial inclusion and economic growth, they are still at risk of multiple cyber security threats, mainly because of human factors [14] [15]. Insufficient employee awareness, social engineering attacks, and insider threats can result in serious data breaches and financial losses, causing these vulnerabilities to occur [16].

Moreover, as mentioned by [10], a large number of MFIs work with restricted resources, preventing them from being able to put in place strong cyber security measures and properly educate their employees. Limited extensive research that specifically looks at the human vulnerabilities that microfinance institutions face in terms of cyber security is creating a crucial gap in understanding the distinct challenges these institutions are up against [11] [17].

According to [13] [14], cyber security for MFIs is made more complex by the changing cyber threats and regulatory requirements they must adhere to. This scenario requires a prompt review of human weaknesses impacting cyber security

in MFIs, the difficulties caused by these weaknesses, and the successful strategies that can be put in place to improve their security status.

1.3. Objectives of the Study

This review aims to explore the human vulnerabilities in cyber security specific to MFIs. It seeks to identify the challenges posed by these vulnerabilities and propose effective solutions. The specific objectives include:

1) Analyzing the current cyber security landscape within MFIs.
2) Identifying specific human vulnerabilities that contribute to cyber threats.
3) Evaluating the effectiveness of existing training and awareness programs.

2. Literature Review

2.1. Understanding the Role of Microfinance Institutions

As per [3] [18], MFIs are described as entities that offer financial services to low-income individuals or those who do not have access to traditional banking services. They go beyond just managing money; their goal is to promote economic growth and reduce poverty [2]. As stated by [19], microfinance institutions cater to a varied customer base, which includes small business owners and low-income individuals [20] [21].

MFIs offer crucial financial services that give power to disadvantaged communities, providing services such as small loans, savings accounts, and programs to improve financial knowledge [22]. The expansion of microfinance institutions in developing nations has significantly grown due to the growing need for convenient financial services, especially among women and marginalized groups [4] [23]. Nevertheless, as these organizations increase their online presence, they must also address the growing risk of cyber security breaches that can disrupt their activities and jeopardize customer confidence [7].

2.2. Cyber Security Landscape and Compliance Issues

The cyber security landscape for MFIs is fraught with challenges, including compliance with regulatory frameworks that mandate the protection of sensitive customer data [24]. The regulatory framework governing cyber security has been evolving, with many governments and relevant authorities recognizing the need for stronger protections against cyber threats [25]. In Kenya, for instance, the Central Bank has established guidelines for financial institutions to enhance their cyber security posture [26].

However, compliance with these regulations can be challenging for MFIs, particularly those with limited resources [27]. The lack of clear guidelines and support for implementing cyber security measures can hinder MFIs' ability to protect sensitive client information and maintain compliance with legal requirements [25]. Furthermore, the dynamic nature of cyber threats necessitates ongoing vigilance and adaptation, which can be difficult for resource-constrained institutions [24] [28].

2.3. Human Vulnerabilities in Cyber Security and MFI

Human vulnerabilities and weaknesses in cyber security are caused by human behavior, like lack of awareness, inadequate training, and vulnerability to manipulation, which heavily result in data and financial breaches of microfinance institutions [15]. Different types of vulnerabilities, like social engineering attacks, insider threats, and insufficient security practices, can emerge [27] [29].

Social engineering attacks use human psychology to trick people into sharing sensitive information. These assaults are especially impactful in MFIs, as staff may be less alert because of the intense work atmosphere [14] [25]. Insider threats occur when employees abuse their privilege to access important data, whether intentionally or accidentally.

The absence of a strong security culture in MFIs can make this problem worse, since employees may not completely grasp the consequences of their actions [25]. A major reason for human vulnerabilities is the inadequate awareness of cyber security by employees [28]. Research indicates that companies with thorough training programs encounter fewer security breaches [18] [30].

2.4. Factors Contributing to Human Vulnerabilities in MFIs

The culture of the organization within MFIs is crucial in influencing how employees view and act towards cyber security. Emphasizing security and promoting transparent discussions about risks can greatly decrease human susceptibilities [27] [30]. On the other hand, a culture that ignores the significance of cyber security or does not offer sufficient training support can worsen weaknesses and raise the chances of security breaches [6].

Training and education for employees are crucial elements of a successful cyber security strategy [3]. Consistent training sessions, including phishing awareness, password management, and data protection, can assist employees in identifying and acting on potential threats [1] [6]. Nevertheless, numerous microfinance institutions find it challenging to dedicate adequate resources to training initiatives, resulting in deficiencies in the knowledge and skills of their staff members [7] [18].

According to [3], continuous investment in training and education is crucial for developing a workforce capable of adapting to the changing cyber security environment. The technology and systems employed by MFIs have the potential to also expose individuals to risks. Obsolete software, insufficient security measures, and system integration gaps can lead to vulnerabilities for cyber-attacks [28].

Additionally, if employees view the technology as burdensome or inefficient, they may be less inclined to follow security protocols [19]. Updating and making technology user-friendly can improve adherence to security protocols and lower the chances of human mistakes [24] [25].

2.5. Challenges Faced by MFIs

Microfinance Institutions (MFIs) face substantial cyber security challenges largely stemming from human vulnerabilities, which make them attractive targets for cy-

bercriminals [24]. One key challenge is social engineering attacks, such as phishing and spear-phishing [27]. These attacks exploit the lack of cyber security awareness among employees, who may unwittingly disclose sensitive information or download malicious software [30].

Since MFIs handle vast amounts of sensitive financial data, a single phishing attack can lead to data breaches, financial theft, or unauthorized access to client information [31]. This vulnerability is exacerbated by a reliance on digital communication for transactions, making it easy for attackers to mimic legitimate requests and gain employees' trust.

Another critical human vulnerability challenge for MFIs is the threat posed by insiders [15]. According to [26], insider threats occur when employees, contractors, or third-party collaborators misuse their access to sensitive information, either intentionally or unintentionally. MFIs often operate in a high-stakes financial environment, making them prone to internal security risks such as fraud, data manipulation, or unauthorized access to client accounts [27].

This can stem from insufficient internal controls or ineffective monitoring mechanisms, which fail to detect or prevent suspicious activities [25]. Additionally, when employees are not properly vetted or cybersecurity policies are loosely enforced, insiders become a severe risk to the organization's cyber security, often with more damaging consequences than external attacks.

The lack of comprehensive cyber security training and a culture of security awareness among employees is another major course of cyber security threat in MFIs [15] [25]. According to [24], many MFIs operate under constrained budgets, which can limit investment in adequate cyber security training programs. As a result, employees may lack essential knowledge of safe online practices, such as identifying phishing attempts, securing passwords, or understanding data protection policies [19].

Without adequate training, employees are ill-equipped to recognize or prevent cyber security threats, significantly increasing the likelihood of breaches. Building a cyber-aware culture is also challenging in MFIs, as it requires continuous education, regular policy updates, and engagement from management to embed security practices into daily operations [14] [25]. This gap in employee education and cultural reinforcement presents a critical obstacle for MFIs aiming to strengthen their cyber resilience.

2.6. Empirical Studies on Human Vulnerabilities vs Cyber Security in MFIs

Studies show that social engineering attacks are among the most prevalent cyber threats targeting financial institutions, including MFIs [13]. Research by Vishwanath, Herath, and Chen [32] revealed that employees in financial institutions often fail to recognize phishing emails, which are commonly used in social engineering attacks. The study found that factors like workload, lack of training, and cognitive biases increase susceptibility to these attacks. These findings suggest that improv-

ing employee awareness and training is essential in reducing vulnerabilities to social engineering, a common challenge for MFIs operating with limited cyber security budgets [11] [12].

Empirical research conducted by Willison and Warkentin [16] focused on insider threats within financial institutions, analyzing case studies to understand how organizational culture and employee access control contribute to insider risks. The study found that weak internal controls and lack of supervision create opportunities for intentional and unintentional insider threats. MFIs, due to their hierarchical structure and focus on accessibility, may struggle to enforce stringent access controls, thus remaining vulnerable to insider threats [27]. This research supports the need for MFIs to establish strict access control policies and regular monitoring to mitigate insider risks [33] [34].

A study by Alavi, Islam, and Iqbal [35] investigated the impact of cyber security awareness training on reducing human errors in small financial institutions, including MFIs. The study surveyed employees from various institutions and found that tailored training programs significantly reduced the likelihood of cyber incidents caused by human error. It also noted that regular training and engagement from top management play a vital role in embedding a culture of cyber security. For MFIs, this research underscores the importance of investing in continuous training and developing a cyber-aware culture, even if resources are limited [17] [36].

These studies collectively highlight the significant role human factors play in cyber security vulnerabilities within MFIs. They emphasize the importance of targeted employee training, robust internal controls, and awareness programs to mitigate risks. The findings from these empirical studies offer a foundational understanding for MFIs aiming to develop more effective strategies to protect against cyber threats.

2.7. Research Gap

Despite valuable insights from existing empirical studies on human vulnerabilities in financial institutions, there remains a research gap in understanding the specific cyber security challenges faced by Microfinance Institutions (MFIs). While current studies touch on social engineering, insider threats, and training in financial contexts, they lack a focused examination of how these vulnerabilities impact MFIs, which operate under unique constraints.

The literature often stresses the importance of employee training and awareness, overlooking the resource constraints that limit MFIs' ability to implement effective programs. Unlike larger institutions, MFIs lack the funds for robust cyber security initiatives, such as up-to-date awareness programs.

Additionally, there is limited research on how organizational culture, regional regulations, and low digital literacy levels among MFI employees influence cyber security risks. Understanding these factors and developing tailored solutions could help MFIs enhance their cyber security posture within their operational re-

alities. Research addressing scalable, cost-effective training and awareness strategies is needed to bridge this gap.

3. Methodology

3.1. Literature Search and Selection

To conduct a comprehensive literature review, relevant academic databases such as Google Scholar, IEEE Xplore, JSTOR, ScienceDirect, and Scopus were utilized. The search focused on peer-reviewed articles, conference papers, reports, and case studies published in the last five years that specifically address human vulnerabilities in cyber security within the context of MFIs. The selection of databases was guided by their relevance to the fields of cyber security, microfinance, and organizational behavior. Each database was searched using specific keywords and phrases related to the topic, ensuring a thorough exploration of the literature [30].

Keywords such as "human factors in cyber security," "cyber security vulnerabilities in MFIs," and "social engineering attacks in microfinance" were employed to identify relevant studies [6]. As an example, the following is the search used in IEEE: TITLE-ABS-KEY (cyber AND security AND human OR vulnerability AND security AND human OR employee AND behavior) AND (cyber AND security AND behavior) AND PUBYEAR > 2019. To increase the precision of the searches, title, abstract and keywords were used as a limiter in all the databases.

The inclusion criteria [37] focused on peer-reviewed sources that directly addressed the topic, while exclusion criteria eliminated non-peer-reviewed articles, those not in English, and studies that did not specifically relate to human vulnerabilities in cyber security within MFIs [38] [39]. The inclusion and exclusion criteria were applied, and for this study, the following criteria are defined:

1) Exclusion criteria

Studies from organization reports, guidelines, technical opinion reports and research design—exclude reviews, editorials and testimonials, as using secondary data would make this review tertiary and non-research literature.

2) Inclusion criteria

Written in English; published in 2019-2023; original studies using theoretical or empirical data; and studies published in Journals, Conference Proceedings and books/book sections.

The focus on studies published between 2019 and 2023 was strategic to ensure that the analysis incorporates the most recent developments and trends in cybersecurity threats and solutions relevant to Microfinance Institutions (MFIs). Cybersecurity is a rapidly evolving field, and this timeframe captures advancements in technology, emerging threats, and regulatory changes that are highly pertinent to addressing human vulnerabilities in cybersecurity for MFIs.

3.2. Data Extraction and Analysis

The selected literature was reviewed and categorized based on themes, including types of human vulnerabilities, challenges specific to MFIs, and solutions and best

practices [6] [40]. Key findings, methodologies, and conclusions were summarized, highlighting similarities, differences, and gaps in the literature [41]. The literature was categorized into distinct themes to facilitate a structured analysis of the findings. This approach allowed for the identification of recurring patterns and themes related to human vulnerabilities and cyber security challenges in MFIs [6].

Each study's key findings were summarized, emphasizing the methodologies employed and the implications of the research for understanding human vulnerabilities in cyber security [28]. A thematic analysis was conducted to identify common patterns and themes that emerged across the literature, providing a comprehensive understanding of the interplay between human factors and cyber security in MFIs [19].

3.3. Critical Evaluation

The quality and rigor of the studies included in the review were evaluated using criteria such as research design, sample size, and data collection methods [6]. This assessment ensured that the findings presented in the review were based on robust and reliable evidence [42]. Gaps in the current literature were identified, highlighting areas where further research is needed to advance the understanding of human vulnerabilities in cyber security within MFIs [18].

3.4. Synthesis of Findings

An integrated framework was developed to combine insights from the literature, addressing human vulnerabilities, challenges, and potential solutions in cyber security for MFIs [6] [31]. Visual representations, such as tables and conceptual diagrams, were utilized to illustrate key themes and relationships identified in the literature [43].

4. Results

4.1. The Identification, Screening, Eligibility and Inclusion Phase

From the analysis, 1357 records were obtained in this study. Before conducting any analysis, the initial step was to eliminate any duplicate entries [44]. A total of 1003 unique records were left after duplicates were removed. As suggested by Weidt and Silva (2016), the initial step in analysis involves screening based on the title and abstract. A total of 849 records were determined to be irrelevant for this review, resulting in 154 articles for further screening.

The second evaluation involved analyzing the introduction and conclusion of each article, depending on the number of articles. In the second screening stage, an evaluation of the methodology section was also incorporated for this research. This reduced the total to 57, with an additional 97 articles being eliminated due to the absence of empirical data and lack of relevance to the topic under review, resulting in a final count of 57 articles for thorough text analysis. Adapted from Page *et al.* [45], the screening process is illustrated in **Figure 1** below.

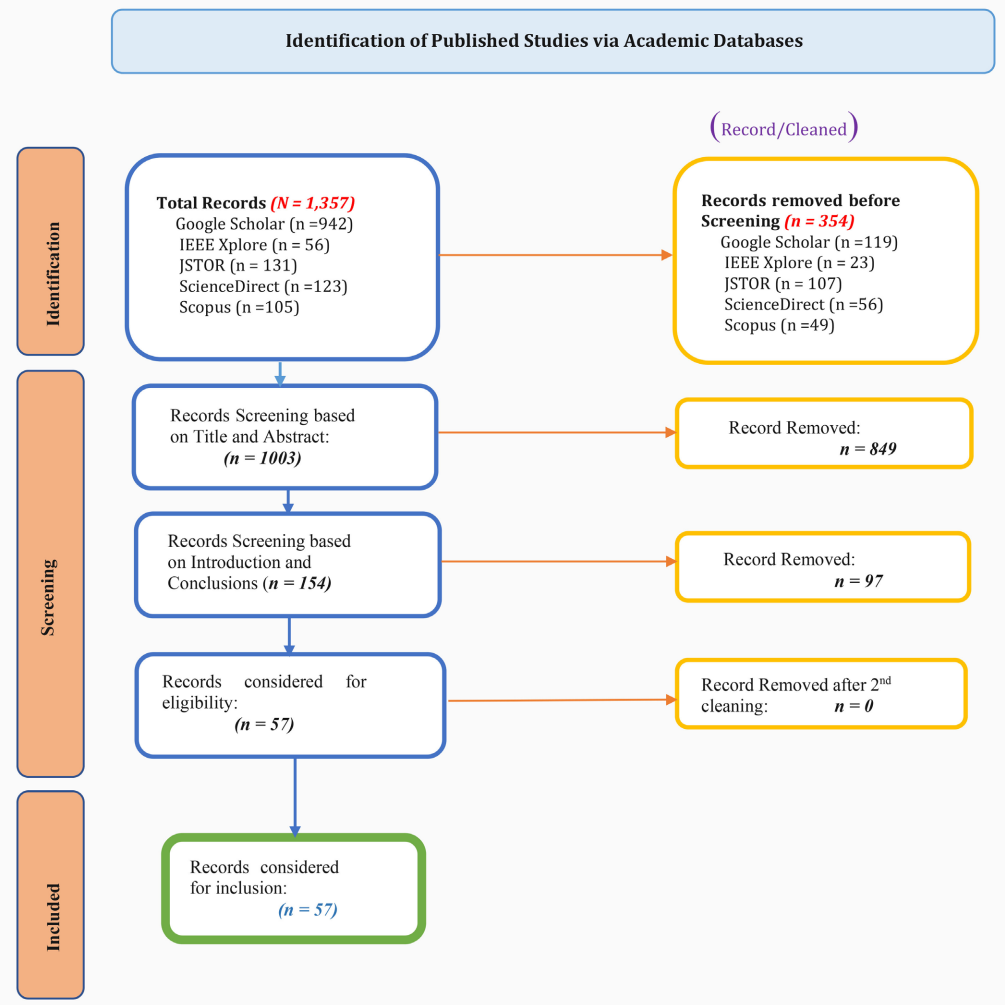

Figure 1. The screening and record inclusion for analysis.

4.2. Trend and Classification of Included Studies

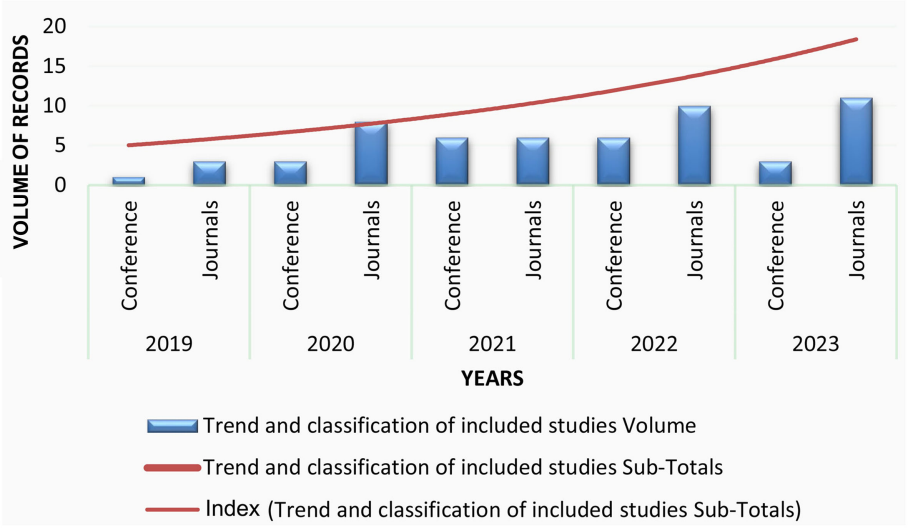

Figure 2. The trend and classification of the included studies.

Of the 57 selected articles, 38 were published in journals, and the remaining 9 in conferences, or 66.67% and 33.33%, respectively as shown in **Figure 2**. The figure also demonstrates the increased interest in the subject in the past two years.

4.3. Findings, Analysis and Discussions

***Objective* 1:** *Analyzing the current cyber security landscape within MFIs*

Analysis of the current cybersecurity landscape in microfinance institutions (MFIs) from the reviewed journals shows a significant prevalence of cyber threats, as 80% of MFIs report having experienced attacks. Phishing and social engineering are the most common threats, recording significant increases of 65% and 40% respectively from 2019 to 2023. Reviews pointed out that cybercriminals often focus on employees with limited cybersecurity knowledge and exploit their weaknesses.

From the 57-reviewed studies in this study, phishing attacks have been increasing at the rate of 20% annually since 2019 and primarily affect inexperienced junior employees who lack knowledge of cybersecurity protocols. Additionally, approximately 15% of microfinance institutions have fallen victim to ransomware attacks focused on accessing sensitive customer data, increasing the risk associated with these organizations. Approximately 70% of microfinance institutions rely on basic antivirus software and firewalls to ensure their security.

Only 30% opt for more sophisticated measures such as multifactor authentication and threat detection systems as pointed out from the 57 review studies. Many microfinance organizations face potential threats from both external and internal sources due to varying levels of security knowledge. One of the studies examining the correlation between implementation of security protocols and attack incidents using regression analysis shows a strong inverse relationship ($R^2 = 0.65$), suggesting that financial institutions with improved protocols are subject to fewer attacks.

***Objective* 2:** *Identifying specific human vulnerabilities that contribute to cyber threats*

In examining specific human vulnerabilities contributing to cyber threats within MFIs, from the 57 reviewed studies for this research, several key issues emerged. Social engineering was identified as the most prevalent vulnerability, with 74% of studies highlighting employees' susceptibility to these tactics. This vulnerability encompasses various manipulative methods, including phishing and impersonation attacks, which exploit employees' trust or lack of awareness. Poor password practices are also common, with about 60% of employees in MFIs reportedly reusing passwords across different systems. The average employee reuses approximately 3.2 score on a scale of 1 to 5 passwords, amplifying the risk of credential-based breaches.

Another significant vulnerability is the lack of adequate security training. A notable 65% of studies cited insufficient training as a contributing factor, with only 40% of MFIs conducting annual training sessions on cyber threats. This lack of regular, focused training leaves many employees underprepared to recognize and

respond to cyber risks effectively.

Vulnerabilities also vary significantly across employee levels. Entry-level employees, due to limited cybersecurity literacy, exhibit the highest vulnerability rate at 78%. Mid-level employees display a 60% susceptibility to social engineering techniques, while management-level employees are primarily vulnerable due to inadequate secure data handling knowledge, with a vulnerability rate of 45%.

***Objective* 3:** *Evaluating the effectiveness of existing training and awareness programs.*

The evaluation of existing training and awareness programs within MFIs reveals varying levels of effectiveness based on the frequency, content, and implementation of these initiatives. Among the MFIs studied, only 35% offer quarterly security training, while 65% either hold annual sessions or lack formal training altogether. MFIs with quarterly training report a 35% lower rate of cyber incidents than those offering only annual sessions, indicating the positive impact of regular training. However, most programs (70%) focus on basic topics, such as password management and phishing awareness, with only 30% covering advanced topics like social engineering defense and incident response. This gap in content scope limits the overall effectiveness of these programs.

In terms of changing employee behavior, frequent training appears to significantly reduce vulnerability to phishing attacks. Employees participating in quarterly sessions showed a 50% decrease in phishing susceptibility, compared to only a 20% reduction among those receiving annual training. Statistical analysis using paired t-tests revealed a substantial reduction in cyber incidents post-training in MFIs that implement frequent and comprehensive training programs ($p < 0.01$), underscoring the value of regular, in-depth training as summarized in Table 1 below.

Table 1. Summary of the findings.

Objective	Key Findings	Statistical Analysis
1. Analyzing the Current Cyber Security Landscape	- 80% of MFIs reported cyber threats, with a 65% increase in phishing and 40% increase in social engineering attacks (2019-2023). - 30% of MFIs use advanced security protocols.	- 20% annual increase in phishing targeting employees. - Regression analysis ($R^2 = 0.65$) shows higher security adoption reduces attack incidents significantly.
2. Identifying Specific Human Vulnerabilities	- 74% of MFIs are vulnerable to social engineering; password reuse is high (60%). - Entry-level employees have the highest vulnerability (78%), mid-level (60%), management (45%).	- ANOVA showed significant vulnerability differences across employee levels ($p < 0.05$).
3. Evaluating Effectiveness of Training Programs	- Only 35% of MFIs provide quarterly training; 65% conduct annual training or none. - Quarterly training reduces phishing susceptibility by 50% vs. 20% for annual training only.	- Paired t-test confirms significant incident reduction post-training ($p < 0.01$).

Awareness program outcomes demonstrate mixed results in knowledge retention and application. From Table 1, while 60% of employees retained their training content well, only 45% consistently applied this knowledge in daily operations,

indicating a disconnect between understanding cybersecurity concepts and practicing them in real scenarios. This gap highlights the need for more interactive, simulation-based training sessions to reinforce practical application. Additionally, cost-effectiveness studies show that MFIs save 1.5 times the cost of implementing security measures per employee by mitigating vulnerabilities through effective training, emphasizing the financial benefit of investing in robust cybersecurity education.

5. Conclusions and Recommendations

5.1. Conclusions

The research indicates that insufficient resources in microfinance institutions (MFIs) affect their capacity to offer thorough training and infrastructure, leading to human vulnerabilities, which is a crucial aspect of cybersecurity risks. Newly hired staff members are vulnerable to cyberattacks due to their lack of knowledge about dangers like phishing and social engineering. Inadequate training prevents the utilization of advanced security measures like multifactor authentication and exposes MFIs to internal and external risks.

Limited funding hampers continued training and the establishment of a robust cybersecurity system. If MFIs do not prioritize strategic training and resource utilization, it could result in continued vulnerabilities in human resources, putting sensitive client data at risk of cyber-attacks. The research emphasizes the importance of enhancing cybersecurity education and funding proactive technologies to reduce risks effectively.

5.2. Recommendations

To build resilience, Microfinance Institutions (MFIs) should implement continuous, cost-effective cybersecurity training tailored to their unique threat landscape. Regular, short training sessions such as monthly or quarterly updates help reinforce cybersecurity skills without overwhelming budgets. This training should focus on critical skills, like phishing awareness and password hygiene, and include simulations to give employees practical experience in identifying threats.

A proactive security culture is equally important for MFIs, starting with leadership support for cybersecurity initiatives and consistent communication about their importance. Establishing open reporting channels for potential threats and encouraging employees to report incidents without fear helps make cybersecurity a shared responsibility. Incentives for good cybersecurity practices and integrating secure habits such as multifactor authentication and routine password updates into daily operations reinforce the mindset that cybersecurity is a fundamental part of the organization's mission.

5.2.1. Recommended Training Cycle and Scope of Proposed Solutions

Training Cycle: Quarterly training sessions are recommended, as MFIs conducting quarterly sessions showed a 35% lower incidence of cyberattacks compared to those holding annual sessions. These sessions should focus on phishing aware-

ness, password hygiene, and recognizing social engineering tactics.

Scope of Solutions

- Enhancing Staff Training Frequency: Regular, simulation-based training to reinforce employee response to phishing and other threats.
- Internal Control Improvements: Implementing robust access control policies, routine monitoring, and multifactor authentication to mitigate insider risks and reduce the scope for negligence.

5.2.2. Scope of Application for Recommendations beyond MFIs

The recommendations outlined for MFIs are highly relevant to small banks due to their analogous operational challenges and resource constraints. Small banks face similar resource constraints as MFIs, making them equally vulnerable to social engineering attacks and insider threats. Quarterly, simulation-based training and robust internal controls can significantly enhance their cybersecurity resilience. Emphasizing multifactor authentication and regular monitoring improves adherence to protocols without high costs. These measures help mitigate human vulnerabilities, reducing exposure to evolving cyber threats. Small banks can adopt these strategies to strengthen security while balancing their limited budgets.

Similarly, credit unions and rural banks, which prioritize financial inclusion, are increasingly exposed to cyber threats due to their reliance on digital platforms and limited digital literacy. Tailored cybersecurity training programs and awareness initiatives are essential to address these risks. Measures like multifactor authentication and proactive cultural changes can protect sensitive client data and maintain regulatory compliance. Regular staff assessments and practical training simulations ensure improved cybersecurity practices. These recommendations help such institutions manage cyber risks effectively while fostering client trust.

5.3. Future Studies

Further studies should explore scalable cybersecurity solutions tailored to resource-limited institutions, focusing on affordable training models and improved internal controls to enhance MFI security resilience.

Expanding the Literature Database and Scope

While databases like IEEE Xplore and Google Scholar for this study provided relevant studies, they might have missed interdisciplinary research from domains such as behavioral psychology or organizational management, which could offer additional insights into human factors in cybersecurity. Expanding the search to databases like PubMed for psychological perspectives or Business Source Complete for management studies could enhance the comprehensiveness of the review. This would provide a more holistic view of vulnerabilities and potential solutions.

Acknowledgements

I would like to express my heartfelt gratitude to my supervisors, Prof. Simon Maina Karume from Kabarak University's Department of Computer Science and

Information Technology and Dr. Alex Kibet from Laikipia University, for their invaluable mentorship and guidance, which greatly influenced my research. I am also grateful to the faculty members of the Cooperative University's Department of Computing and Informatics, particularly Prof. J. M. Kihoro, Doctors. Mbandu, Katila, Omollo, Mile, and Muriuki, for their support and encouragement. My classmates, Gilly Gathogo, Mike, George, Dangote, and Beatrice, provided insightful discussions and encouragement throughout this journey. Finally, I want to express my heartfelt gratitude to my husband, Zachariah Kimani, and my family for their unwavering love and support throughout this rewarding experience.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Joseph, O.O. and Kibera, F. (2019) Organizational Culture and Performance: Evidence from Microfinance Institutions in Kenya. *Sage Open*, **9**. https://doi.org/10.1177/2158244019835934

[2] Wairimu, Z. and Mwilaria, S.M. (2017) Microfinance Institutions' Social Intermediation and Micro and Small Enterprises Survival in Thika Town, Kenya. *Asia Pacific Journal of Multidisciplinary Research*, **5**, 87-93. https://www.apjmr.com

[3] Kiganda, M. (2022) An Assessment of the Factors Affecting Cyber Resilience in Micro-Finance Institutions. https://su-plus.strathmore.edu/handle/11071/12982

[4] Mohamed, E. (2024) Measuring the Effects of Digital Transformation on Organisational Performance: A Case Study of Microfinance Institutions. In: Carter, S.D. and Bensal, S., Eds., *Management and Resilience of African Organizations in Times of Crisis*, Springer, 125-142. https://doi.org/10.1007/978-3-031-56007-1_8

[5] Wu, Y., Xie, Z., Ji, S., Liu, Z., Zhang, X., Lin, C., *et al.* (2023) Fraud-Agents Detection in Online Microfinance: A Large-Scale Empirical Study. *IEEE Transactions on Dependable and Secure Computing*, **20**, 1169-1185. https://doi.org/10.1109/tdsc.2022.3151132

[6] Limna, P., Kraiwanit, T. and Siripipattanakul, S. (2023) The Relationship between Cyber Security Knowledge, Awareness and Behavioural Choice Protection among Mobile Banking Users in Thailand. *International Journal of Computing Sciences Research*, **7**, 1133-1151. https://doi.org/10.25147/ijcsr.2017.001.1.123

[7] Abdullah, W.M.Z.B.W., Zainudin, W.N.R.A.B., Ismail, S.B. and Zia-ul-haq, H.M. (2022) The Impact of Microfinance Services on Malaysian B40 Households' Socioeconomic Performance: A Moderated Mediation Analysis. *International Journal of Sustainable Development and Planning*, **17**, 1983-1996. https://doi.org/10.18280/ijsdp.170634

[8] Wong, L., Lee, V., Tan, G.W., Ooi, K. and Sohal, A. (2022) The Role of Cybersecurity and Policy Awareness in Shifting Employee Compliance Attitudes: Building Supply Chain Capabilities. *International Journal of Information Management*, **66**, Article ID: 102520. https://doi.org/10.1016/j.ijinfomgt.2022.102520

[9] Onumo, A., Ullah-Awan, I. and Cullen, A. (2021) Assessing the Moderating Effect of Security Technologies on Employees Compliance with Cybersecurity Control Procedures. *ACM Transactions on Management Information Systems*, **12**, 1-29. https://doi.org/10.1145/3424282

[10] Ewool, L.M. and Quartey, J.A. (2021) Evaluation of the Effect of Risk Management Practices on the Performance of Microfinance Institutions. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, **11**, 211-241. https://doi.org/10.6007/ijarafms/v11-i1/8440

[11] Hijji, M. and Alam, G. (2022) Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. *Sensors*, **22**, Article No. 8663. https://doi.org/10.3390/s22228663

[12] Al-Mohannadi, H., Awan, I., Al Hamar, J., Al Hamar, Y., Shah, M. and Musa, A. (2018) Understanding Awareness of Cyber Security Threat among IT Employees. 2018 6*th International Conference on Future Internet of Things and Cloud Workshops* (*FiCloudW*), Barcelona, 6-8 August 2018, 188-192. https://doi.org/10.1109/w-ficloud.2018.00036

[13] Siddiqi, M.A., Pak, W. and Siddiqi, M.A. (2022) A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. *Applied Sciences*, **12**, Article No. 6042. https://doi.org/10.3390/app12126042

[14] Hartarska, V. and Cull, R.J. (2023) Handbook of Microfinance, Financial Inclusion and Development. Edward Elgar Publishing.

[15] Al Aamer, A.K. and Hamdan, A. (2023) Cyber Security Awareness and SMEs' Profitability and Continuity: Literature Review. In: El Khoury, R. and Nasrallah, N., Eds., *Contributions to Management Science*, Springer, 593-604. https://doi.org/10.1007/978-981-99-6101-6_43

[16] Willison, R., Warkentin, M. and Johnston, A.C. (2016) Examining Employee Computer Abuse Intentions: Insights from Justice, Deterrence and Neutralization Perspectives. *Information Systems Journal*, **28**, 266-293. https://doi.org/10.1111/isj.12129

[17] Dube, H. and Kwenda, F. (2023) Credit Risk Management and the Financial Performance of Microfinance Institutions in Southern Africa. *The Journal of Developing Areas*, **57**, 145-157. https://doi.org/10.1353/jda.2023.0026

[18] Rasel, M.A. and Win, S. (2020) Microfinance Governance: A Systematic Review and Future Research Directions. *Journal of Economic Studies*, **47**, 1811-1847. https://doi.org/10.1108/jes-03-2019-0109

[19] Boadi Joseph, M., Bondinuba, F.K., Eyiah, A.L. and DeGraft, O.-M. (2019) Modeling the Relationship between Risks and the Sustainability of Microfinance Institutions (MFIs) in Ghana. *Journal of Economics and Sustainable Development*, **10**, 103-119.

[20] European Digital SME Alliance (2020) The EU Cybersecurity Act and the Role of Standards for SMEs-Position Paper.

[21] Jayeola, O., Sidek, S., Sanyal, S., Hasan, S.I., An, N.B., Mofoluwa Ajibade, S., *et al.* (2022) Government Financial Support and Financial Performance of SMEs: A Dual Sequential Mediator Approach. *Heliyon*, **8**, e11351. https://doi.org/10.1016/j.heliyon.2022.e11351

[22] Mwangi, B.J. and Brown, I. (2014) A Decision Model of Kenyan SMEs' Consumer Choice Behavior in Relation to Registration for a Mobile Banking Service: A Contextual Perspective. *Information Technology for Development*, **21**, 229-252. https://doi.org/10.1080/02681102.2013.874320

[23] Omondi, R.I.A. and Jagongo, A. (2018) Microfinance Services and Financial Performance of Small and Medium Enterprises; Case of Kilifi Town in Kenya. *International Academic Journal of Economics and Finance*, **3**, 24-43. https://www.iajournals.org/articles/iajef_v3_i1_24_43.pdf

[24] Miryala, N.K. and Gupta, D. (2022) Data Security Challenges and Industry Trends. *International Journal of Advanced Research in Computer and Communication Engineering*, **11**, 300-310. https://doi.org/10.17148/ijarcce.2022.111160

[25] Bahuguna, A., Bisht, R.K. and Pande, J. (2020) Country-Level Cybersecurity Posture Assessment: Study and Analysis of Practices. *Information Security Journal: A Global Perspective*, **29**, 250-266. https://doi.org/10.1080/19393555.2020.1767239

[26] Ralarala, S. (2020) The Impact of Cybercrime on e-Commerce and Regulation in Kenya, South Africa and the United Kingdom. Strathmore University.

[27] Mphatheni, M.R. and Maluleke, W. (2022) Cybersecurity as a Response to Combating Cybercrime. *International Journal of Research in Business and Social Science*, **11**, 384-396. https://doi.org/10.20525/ijrbs.v11i4.1714

[28] Tawina, C. (2023) Analyzing Cybersecurity Issues Associated with Mobile Money Usage in Malawi. Ashesi University College.

[29] Voola, A.P. (2019) Gendered Vulnerabilities in Australian Microfinance. *Social Business*, **9**, 29-47. https://doi.org/10.1362/204440819x15504844628056

[30] Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P. and Hur, J. (2024) Cybersecurity Threats in Fintech: A Systematic Review. *Expert Systems with Applications*, **241**, Article ID: 122697. https://doi.org/10.1016/j.eswa.2023.122697

[31] Al-Sanjrae, A.A. and Al-Nuaimi, Z.A. (2022) Financial Depth and Its Impact on Financial Inclusion by Applying to Iraq and Egypt. *Tanmiyat al-Rafidain*, **41**, 133-160.

[32] Vishwanath, A., Harrison, B. and Ng, Y.J. (2016) Suspicion, Cognition, and Automaticity Model of Phishing Susceptibility. *Communication Research*, **45**, 1146-1166. https://doi.org/10.1177/0093650215627483

[33] Savaş, S. and Karataş, S. (2022) Cyber Governance Studies in Ensuring Cybersecurity: An Overview of Cybersecurity Governance. *International Cybersecurity Law Review*, **3**, 7-34. https://doi.org/10.1365/s43439-021-00045-4

[34] Conteh, N.Y. and Schmick, P.J. (2016) Cybersecurity: Risks, Vulnerabilities and Countermeasures to Prevent Social Engineering Attacks. *International Journal of Advanced Computer Research*, **6**, 31-38. https://doi.org/10.19101/ijacr.2016.623006

[35] Iqbal, M., Siti Astuti, E., Trialih, R., Wilopo, Arifin, Z. and Alief Aprilian, Y. (2020) The Influences of Information Technology Resources on Knowledge Management Capabilities: Organizational Culture as Mediator Variable. *Human Systems Management*, **39**, 129-139. https://doi.org/10.3233/hsm-190562

[36] Gomera, W.C. (2020) The Use of Mobile Technology to Enhance the Interaction between Microfinance Institutions and Micro Businesses in the Tanzanian Context. University of Eastern Finland.

[37] Kumarage, A.M. (2018) From Exclusion to Inclusion: Evolution of the Role of Hansards in the Interpretative Process. https://ssrn.com/abstract=3599972

[38] Hausstätter, R.S. (2013) In Support of Unfinished Inclusion. *Scandinavian Journal of Educational Research*, **58**, 424-434. https://doi.org/10.1080/00313831.2013.773553

[39] Wilhoit Larson, E., Linabary, J.R. and Long, Z. (2022) Communicating Inclusion: A Review and Research Agenda on Inclusion Research in Organizational Communication. *Annals of the International Communication Association*, **46**, 63-90. https://doi.org/10.1080/23808985.2022.2069045

[40] Vignau, B., Clemente, P. and Berthomé, P. (2024) Systematic Literature Review: References Extraction Helper and Automatic Analysis. *Software Impacts*, **21**, Article ID: 100669. https://doi.org/10.1016/j.simpa.2024.100669

[41] Cheloff, A.Z., Pochapin, M.B. and Popov, V. (2024) Su1981 Potential of Generative

AI in Meta-Analysis: Automating Literature Review and Data Extraction. *Gastroenterology*, **166**, S-890. https://doi.org/10.1016/s0016-5085(24)02530-7

[42] Lai, J.W.M. and Bower, M. (2019) Evaluation of Technology Use in Education: Findings from a Critical Analysis of Systematic Literature Reviews. *Journal of Computer Assisted Learning*, **36**, 241-259. https://doi.org/10.1111/jcal.12412

[43] Adu, K.K., Patrick, N., Park, E.G. and Adjei, E. (2018) Evaluation of the Implementation of Electronic Government in Ghana. *Information Polity*, **23**, 81-94. https://doi.org/10.3233/ip-170420

[44] Skarlatidou, A., Hamilton, A., Vitos, M. and Haklay, M. (2019) What Do Volunteers Want from Citizen Science Technologies? A Systematic Literature Review and Best Practice Guidelines. *Journal of Science Communication*, **18**, A02. https://doi.org/10.22323/2.18010202

[45] Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., *et al.* (2021) The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *BMJ*, **123**, n71. https://doi.org/10.1136/bmj.n71