Scientific Research Publishing

Open Journal of Applied Sciences, 2026, 16(2), 696-717
https://www.scirp.org/journal/ojapps
ISSN Online: 2165-3925
ISSN Print: 2165-3917

Assessing Human-Induced Cybersecurity Risk Using a Human Vulnerabilities Exposure Index (CSHVEI)

Alex Kibet

Faculty of Science and Applied Technology, Department of Computing and Informatics, Laikipia University, Nyahururu, Kenya
Email: alexriongosha@gmail.com

How to cite this paper: Kibet, A. (2026) Assessing Human-Induced Cybersecurity Risk Using a Human Vulnerabilities Exposure Index (CSHVEI). *Open Journal of Applied Sciences*, **16**, 696-717.
https://doi.org/10.4236/ojapps.2026.162043

Received: September 3, 2025
Accepted: February 24, 2026
Published: February 27, 2026

Abstract

Cybersecurity resilience is widely understood to rest on the integration of people, processes, and technology. However, existing cybersecurity research and practice have largely prioritized technological controls and procedural safeguards, often underestimating the human factor, which consistently represents the most exploited point of attack. This study addresses this gap by developing a comprehensive and quantifiable model for assessing human-induced cybersecurity risks. The paper introduces the Cybersecurity Human Vulnerabilities Exposure Index (CSHVEI), a novel framework designed to measure and operationalize human-related cyber exposure within Microfinance Institutions (MFIs) in Nairobi County, Kenya. Building on a critical review of existing cybersecurity exposure models and standards, including ISO/IEC 27001 and the NIST Cybersecurity Framework, the study identifies key limitations in capturing human-centric vulnerabilities. To address these shortcomings, the CSHVEI categorizes human-induced risks into three core domains: human error, ignorance, and negligence. Using a mixed-methods approach, the study integrates an integrative literature review with empirical survey data to derive, validate, and weight the index components. Statistical analyses confirm the significant contribution of all three vulnerability domains to overall cybersecurity exposure, with negligence emerging as the strongest predictor. The model is further operationalized through a prototype system that demonstrates practical application, enabling organizations to compute exposure scores, visualize risk levels, and generate targeted mitigation recommendations. The findings demonstrate that human behavior is a dominant determinant of cybersecurity exposure in MFIs, often overriding the presence of technical controls. By translating human vulnerabilities into measurable exposure metrics, the CSHVEI provides organizations and policymakers with an evidence-based tool to assess, compare, and manage human-centric cybersecurity risks, thereby strengthening organiza-

tional resilience and informed decision-making.

Keywords

Human Factors, MFIs, Cyber-Security, Attack Surface, Exposure Index, Framework, Model

1. Introduction

The rapid digitization of organizational operations across both public and private sectors has significantly expanded the cyber-attack surface, exposing institutions to increasingly sophisticated and human-centric cyber threats [1] [2]. While advancements in cybersecurity technologies have strengthened perimeter defenses, empirical evidence consistently demonstrates that human behavior remains the most exploited vulnerability in contemporary cyber incidents [3]. Cyber adversaries increasingly bypass technical safeguards by targeting human weaknesses such as negligence, insufficient awareness, trust exploitation, and procedural non-compliance [4].

Recent studies in the Kenyan and broader Global South context highlight that technology-driven governance systems often fail not because of weak architectures, but due to deficiencies in human interaction, oversight, and accountability mechanisms. For instance, blockchain-based governance research shows that even systems designed to enhance transparency and trust are vulnerable when human actors interact with them through flawed processes, weak enforcement, or inadequate institutional coordination [5]. These findings underscore the reality that secure digital infrastructures alone are insufficient without parallel mechanisms to address human-induced risks.

In the financial sector, particularly within Microfinance Institutions (MFIs), these vulnerabilities are amplified by constrained resources, rapid digital adoption, and high reliance on staff-mediated processes [6]. A comprehensive review of human vulnerabilities in MFIs identifies social engineering, insider threats, and inadequate cybersecurity awareness as dominant contributors to cyber exposure, accounting for most reported incidents [7]-[9]. These findings align with global trends indicating that human factors now constitute the primary attack vector across financial institutions, surpassing purely technical exploits.

Beyond cybersecurity, blockchain-based system design research further illustrates how governance opacity, limited stakeholder participation, and weak incentive alignment can intensify systemic risk, even in technologically advanced platforms. Design Science studies on blockchain governance architectures demonstrate that transparency, accountability, and security outcomes depend heavily on how human roles, incentives, and decision-making structures are operationalized within digital systems [10]-[13]. This reinforces the argument that human behavior is not merely an external risk factor but an integral component of system se-

curity and resilience.

Earlier blockchain research focusing on smart contracts and decentralized architectures similarly emphasizes that immutability and decentralization do not automatically guarantee trust or security. Instead, poor configuration, misuse, or inadequate human oversight can introduce new vulnerabilities, particularly in environments handling sensitive financial or personal data [14] [15]. These insights are critical for understanding why organizations with robust technical controls continue to experience high breach rates.

Despite growing recognition of the human factor in cybersecurity, existing frameworks and exposure models largely remain technology-centric, offering limited mechanisms for systematically measuring, weighting, and operationalizing human-induced vulnerabilities. While standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework acknowledge the importance of people, they stop short of providing quantitative tools to assess human exposure levels within organizational contexts [8].

This study addresses this gap by developing a Cybersecurity Human Vulnerabilities Exposure Index (CSHVEI), specifically tailored to Microfinance Institutions in Nairobi County, Kenya. Drawing on empirical evidence and prior governance and cybersecurity research, the proposed model translates human behavior, awareness, and compliance into measurable exposure components. By categorizing vulnerabilities into human error, ignorance, and negligence, the CSHVEI provides a structured, evidence-based mechanism for quantifying human-induced cyber risk and supporting informed decision-making.

Statement of the Problem

Cybersecurity resilience is fundamentally anchored on the integration of people, processes, and technology. Despite this widely accepted triad, contemporary cybersecurity research and organizational practice remain disproportionately focused on technological controls and procedural safeguards, with limited attention given to the human factor. Empirical evidence consistently demonstrates that human behavior through error, negligence, and insufficient awareness constitutes the most frequently exploited vector in cyber incidents across sectors.

Organizations continue to invest heavily in advanced security technologies. However, cybersecurity breaches persist largely because human-induced vulnerabilities enable attackers to bypass technical defenses. Operational errors, procedural non-compliance, weak cybersecurity awareness, and poor security culture significantly elevate organizational exposure, particularly in environments where staff interact directly with digital systems and sensitive data. Microfinance Institutions are especially vulnerable due to rapid digital transformation, constrained resources, and heavy reliance on staff-mediated processes.

Although the significance of human factors in cybersecurity is increasingly acknowledged, existing cybersecurity frameworks and exposure models provide limited mechanisms for systematically measuring and quantifying human-related

vulnerabilities. Most current approaches remain technology-centric and lack structured, data-driven tools capable of translating human behavior into measurable exposure indicators. Consequently, organizations lack actionable metrics to identify, compare, and prioritize human-induced risks or to evaluate the effectiveness of mitigation interventions.

This gap necessitates the development of a robust, context-sensitive model capable of quantitatively assessing human-related cybersecurity exposure. In response, this study seeks to develop a Cybersecurity Human Vulnerabilities Exposure Index (CSHVEI) that systematically measures the impact of human error, ignorance, and negligence on cybersecurity exposure within Microfinance Institutions. By operationalizing human behavior into measurable exposure components, the study aims to support evidence-based risk management, informed decision-making, and enhanced organizational cybersecurity resilience.

2. Literature Review

2.1. The Pivotal Role of Human Factors in Cybersecurity

Contemporary cybersecurity threats have evolved beyond strictly technical flaws, increasingly arising from the interplay between human behaviour and technological systems. Although traditional frameworks prioritised technological safeguards within the confidentiality-integrity-availability (CIA) model, substantial evidence shows that human actors represent both the strongest protective asset and the most frequently exploited point of compromise [16] [17]. This shift reframes organizational security as a socio-technical construct in which behavioural factors critically shape security performance.

The financial sector particularly microfinance institutions operating with extensive digital services, yet constrained security budgets illustrate this heightened exposure. The *2025 Kenya Cybersecurity Report* notes the escalation in social engineering incidents targeting financial personnel, especially through phishing schemes [18]. This mirrors global developments in which adversaries circumvent robust technical controls by leveraging psychological manipulation techniques such as authority cues, urgency framing, and trust exploitation [19], thereby compromising even well-trained staff.

Within organizations, human susceptibility typically emerges through insufficient security knowledge, weak motivation to comply with protocols, and inherent cognitive limitations. [20] report that unintentional insider threats, stemming from errors or negligence, constitute roughly 68% of incidents in environments with limited security capacity. Similarly, the *2023 Verizon Data Breach Investigations Report* attributes 74% of breaches to the human element, frequently via credential theft, phishing, and business email compromise. Collectively, these patterns highlight the necessity for sector-specific tools capable of systematically measuring human-centred vulnerabilities in financial institutions.

2.2. Human Factors in Cybersecurity

Cybersecurity addresses both digital vulnerabilities and the strategies to mitigate them. The success of cyberattacks depends on attackers' prior knowledge and information acquired during the attack [3]. Its core objective is to protect the confidentiality, integrity, and availability of computing resources across organizational networks. While traditional approaches focus on technical defenses, encryption, network protections, and algorithms, scholars emphasize that cybersecurity also entails the interplay among data, systems, and human actors [21]. Without this multidisciplinary perspective, technical measures remain insufficient, as evidenced by the persistent rise in cyber incidents [22].

2.2.1. Cybersecurity Awareness

Cybersecurity awareness, which hinges on employees' comprehension of cybersecurity risks, stands as a cornerstone. Well-informed personnel are better equipped to identify and appropriately respond to security threats. Consistent cybersecurity training and awareness programs serve as potent tools for enhancing this factor [23].

2.2.2. User Behaviour

Moreover, human behavior can either fortify or undermine cybersecurity. Employees' actions, such as inadvertently clicking on phishing emails, sharing passwords, or downloading malicious files, can open the door to vulnerabilities. Therefore, it's imperative to ensure that employees adhere to security policies and best practices [24].

2.2.3. Password Management

Password management is another critical human factor. Weak passwords, password sharing, and infrequent updates pose common human-related security risks. Promoting robust password policies and encouraging the use of password management tools can effectively mitigate these issues [25].

2.2.4. Social Engineering

Social engineering is a major cybersecurity vulnerability because it exploits human psychology, trust, curiosity, and helpfulness, to obtain confidential information or induce harmful actions. Techniques include phishing, pretexting, baiting, and tailgating, all of which bypass technological defences by targeting human behaviour, making detection difficult.

Mitigating these threats requires a combination of education, technology, and policy. Employee awareness programs help identify suspicious requests, while advanced email filtering and Multi-Factor Authentication (MFA) block unauthorized access. Clear security policies and effective incident response plans ensure prompt mitigation of attacks. Together, these measures strengthen organizational resilience and highlight the importance of continuous vigilance in cybersecurity [9].

2.2.5. Insider Threats

Insider threats represent a critical human-related cybersecurity risk, arising from individuals within an organization who have privileged access to systems, networks, and data [26]. These threats can be classified as malicious insiders who intentionally steal data, sabotage systems, or engage in espionage and unintentional insiders who inadvertently cause security breaches through actions like falling for phishing attacks, negligence, or errors that expose vulnerabilities. Malicious insiders are particularly difficult to detect and prevent due to their knowledge of internal systems, while unintentional insiders pose ongoing risks that cannot be quickly eliminated.

Mitigating insider threats requires a multi-layered approach combining technical controls, procedural safeguards, and human-focused interventions [27]. Key measures include role-based access control (RBAC) to restrict privileges, continuous monitoring with Security Information and Event Management (SIEM) systems, and user behavior analytics to detect deviations from normal activity. Complementary strategies involve employee training, awareness programs, and robust incident response plans for rapid containment and remediation. Together, these measures strengthen organizational resilience and reduce both the likelihood and impact of insider threats.

2.2.6. Outsider Threats

Outsider threats arise from external factors such as hackers, ransomware attackers, and unidentified individuals, posing significant risks to organizations, governments, and healthcare institutions [28]. The severity of these threats depends on attackers' motivations and methods, ranging from financially driven attacks to hacktivist campaigns that steal information before causing operational or reputational damage. Mitigation strategies include regular system updates, staff training, and deployment of cybersecurity tools like firewalls, web gateways, and network detection and response solutions [29].

These threats are also classified as direct, exploiting vulnerabilities immediately, or indirect, leading to breaches over time [30]. Ulven's multi-dimensional model further categorizes threats by source, agents, motivation, objectives, and impact, providing a comprehensive framework for understanding cybersecurity risks [31].

2.2.7. Human Error

Human errors are a critical human-factor risk in cybersecurity, arising from inadvertent actions or oversights such as system misconfigurations, accidental data leaks, or failure to apply security updates [32]. These errors, though unintentional, can lead to serious consequences including data breaches, system vulnerabilities, and unauthorized access.

Mitigation requires proactive organizational measures. Regular employee training and awareness programs help prevent common mistakes, while automated security checks and validation processes detect misconfigurations before exploitation. Clear, documented procedures for updates and patches further reduce risk.

Encouraging a culture of accountability and prompt error reporting ensures timely corrective action. Together, these strategies enhance resilience and minimize vulnerabilities associated with human error [32].

2.3. Impact of Human Factors in Cyber Security

Human factors significantly influence cybersecurity risk. In the United States, 83% of retailers are exposed to vulnerabilities, making customer data a prime target for cyberattacks in the e-commerce sector [3]. Attackers employ techniques such as malware, ransomware, phishing, e-skimming, and distributed denial-of-service attacks, highlighting that technological adoption brings both opportunities and security challenges.

Security breaches are increasingly common; surveys show that breaches affect 81% - 90% of large organizations. Human error remains a major contributor: 71% of breaches result from inadvertent employee mistakes, 68% from negligence, and 61% from malicious insider actions [33]. Cybercriminals now target human vulnerabilities, trust, helpfulness, and personal or cultural traits, rather than machines, underscoring the central role of human behaviour in cybersecurity risk [34].

2.4. Existing Frameworks and Models for Human Vulnerability Assessment

According to [9], most cybersecurity frameworks emphasize technical controls while under-addressing human-factor exposure. [15] similarly notes that organizations tend to prioritize technology over human behaviour, despite evidence that human weaknesses account for most cyber incidents. This review responds directly to examiners' recommendations by expanding coverage beyond general frameworks to include models specifically addressing human vulnerabilities.

3. Material and Methods

This study employs a mixed-method research approach guided by the following research questions:

What human-factor vulnerabilities significantly contribute to cybersecurity exposure within MFIs?

How can these human-factor vulnerabilities be systematically categorized and operationalized into measurable components suitable for an exposure index in MFIs?

How can a Cybersecurity Human Vulnerabilities Exposure Index (CSHVEI) be developed, refined, and validated for practical application across MFIs?

The research begins with an Integrative Literature Review (ILR), chosen for its capacity to synthesize evidence from diverse sources, including empirical studies, conceptual frameworks, policy documents, and organizational reports. This phase enables a comprehensive identification of human-factor vulnerabilities that inform the initial structure and constructs of the CSHVEI model.

Following the ILR, the study incorporates mixed-method procedures to refine and validate the emerging model. Qualitative insights from organizational contexts support the interpretation and classification of human vulnerability indicators, while quantitative data collected through a descriptive survey provide the basis for measurement, weighting, and empirical verification of the index components. The survey results allow the model to be tested for coherence, relevance, and applicability across varying organizational environments.

This methodological design ensures that the CSHVEI is conceptually grounded, systematically developed, and empirically strengthened, offering a practical and evidence-based tool for assessing human-induced cybersecurity exposure.

3.1. Model Development Approach

3.1.1. Derivation of the CSHVEI Formula

To systematically assess human-induced cybersecurity risks, this study proposes a hybrid Human Factor Index that combines ISO 27001 and the NIST Cybersecurity Framework (CSF). This integration leverages ISO 27001's detailed control objectives and NIST CSF's actionable functions to provide a holistic view of human vulnerabilities and organizational security culture.

Key human factor considerations include policy implementation, organizational structure, personnel security, asset management, access control, physical and environmental protection, operations security, and incident management. The mapping of these elements to NIST's governance, identify, protect, detect, respond, and recover functions forms the basis for deriving the CSHVEI formula. Tailored questionnaires operationalize these variables into measurable components, providing the foundation for a mathematically robust index.

3.1.2. Factor Reduction

To improve interpretability and reduce complexity, the CSHVEI variables were consolidated into three core categories of human vulnerabilities:

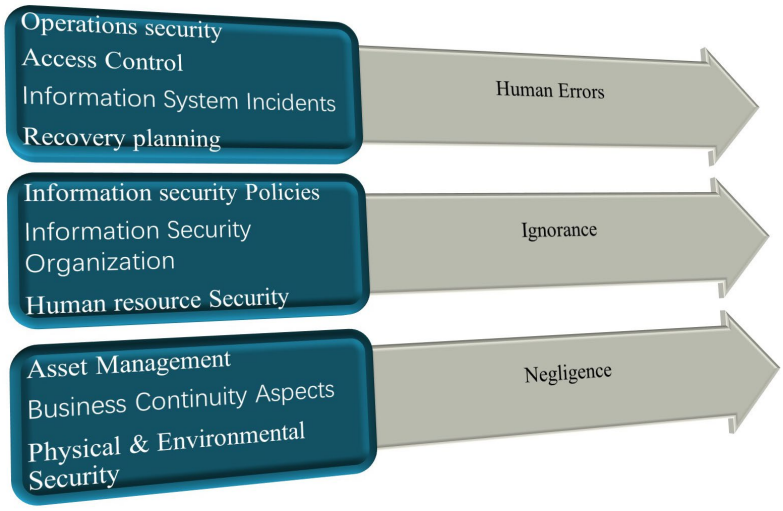


Figure 1. CSHVEI factor reduction.

1) Human Errors: Inadvertent mistakes such as operational lapses, access control errors, mishandling security incidents, or flawed recovery procedures.

2) Ignorance: Knowledge gaps and insufficient awareness, leading to poor application of security policies, unclear understanding of organizational roles, and inadequate personnel training.

3) Negligence: Failure to follow security procedures, including mismanagement of assets, inadequate physical security, and insufficient business continuity planning.

This reduction focuses assessment, reduces noise, and allows organizations to better understand and prioritize their human-related cybersecurity risks. Figure 1 shows CSHVEI Factor Reduction.

3.1.3. Prototype Implementation

The CSHVEI model was operationalized through a prototype system, designed with modules for:

1) User Authentication: Ensuring only authorized users can access the system.

2) Posture Input: Collecting user-provided cybersecurity posture information.

3) Information Processing: Calculating CSHVEI scores using weighted variables.

4) Record Management: Storing historical posture data and weights.

5) Visualization & Reporting: Displaying scores and actionable recommendations.

The prototype demonstrates how the index can be applied in real-world organizational settings, enabling continuous monitoring, evaluation, and mitigation of human-induced cybersecurity vulnerabilities. Figure 2 illustrates functionality of the prototype.

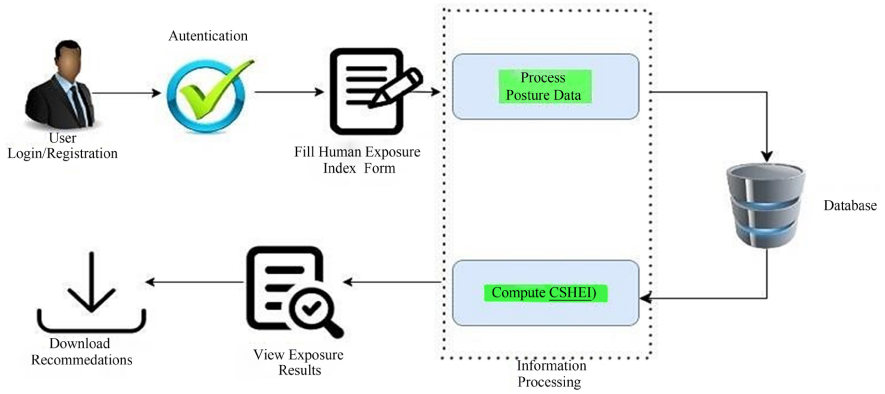


Figure 2. Framework for implementation CSHVEI.

The implementation of the model was realized through the following technologies; Hypertext pre-processor (PHP) as server-side programming language to handle the logic and interface with the database, bootstrap 4 to manage front-end styles and layout, MySQL database management system, and JavaScript and JQuery to add response to the system specially the metric gauges and modals. The follow-

ing sections present different modules developed through for the model.

3.1.4. Registration Module

The module allows the microfinance institution (MFI) user to register their details and credentials that will permit them to use the model. This is accessible through register link on the index page and prompts the user to fill the details as indicated in Figure 3. A dully filled MFI registration form saves the details of the user to MySQL database upon submission. Security measures are applied at this stage through proper validation that is done for email, size of phone numbers and passwords which are hashed before they are saved to the database. Figure 4 shows the user and admin log in pages after registration.

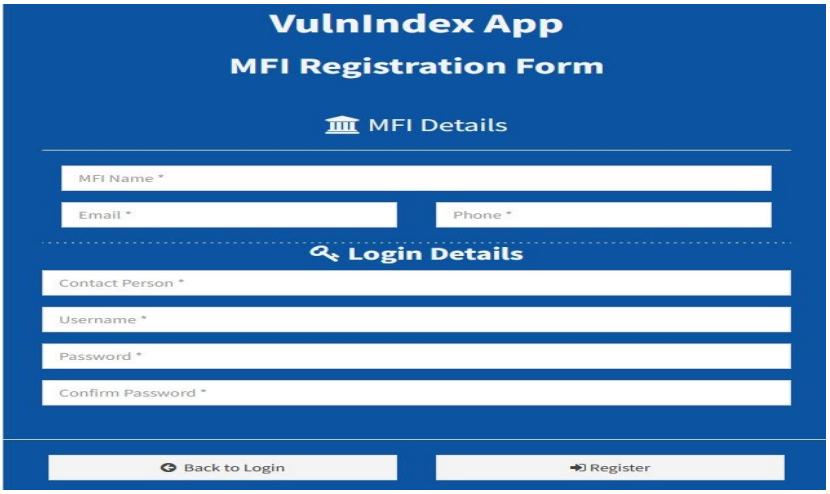


Figure 3. User registration.

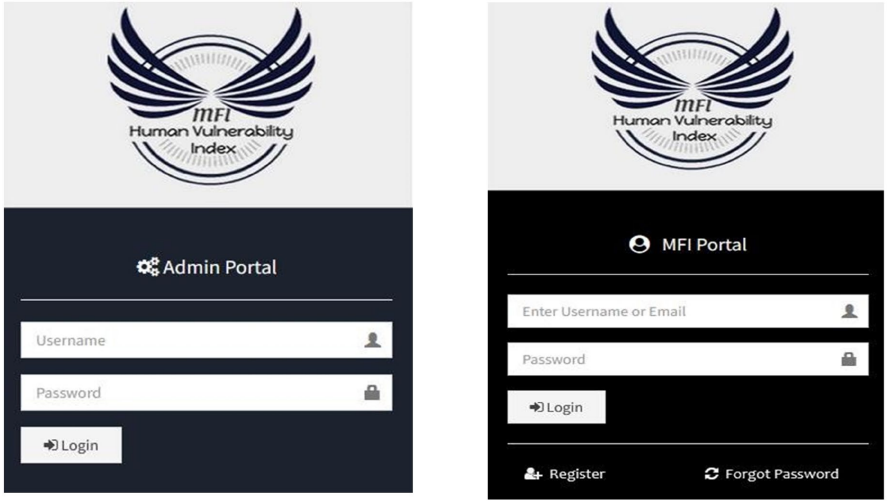


Figure 4. User and admin log in modules.

3.1.5. MFI Dashboard

The MFI User is directed to MFI dashboard when they are successfully authenticated at the login. The dashboard displays basic information about the system

such as human vulnerability scores and maturity indices, the level of MFI human vulnerability derived as a mean score of the user scores for all assessment questions, the number of recommendations that the MFI has to improve the maturity score and the MFI score distribution chart. Figure 5 shows the user dashboard.

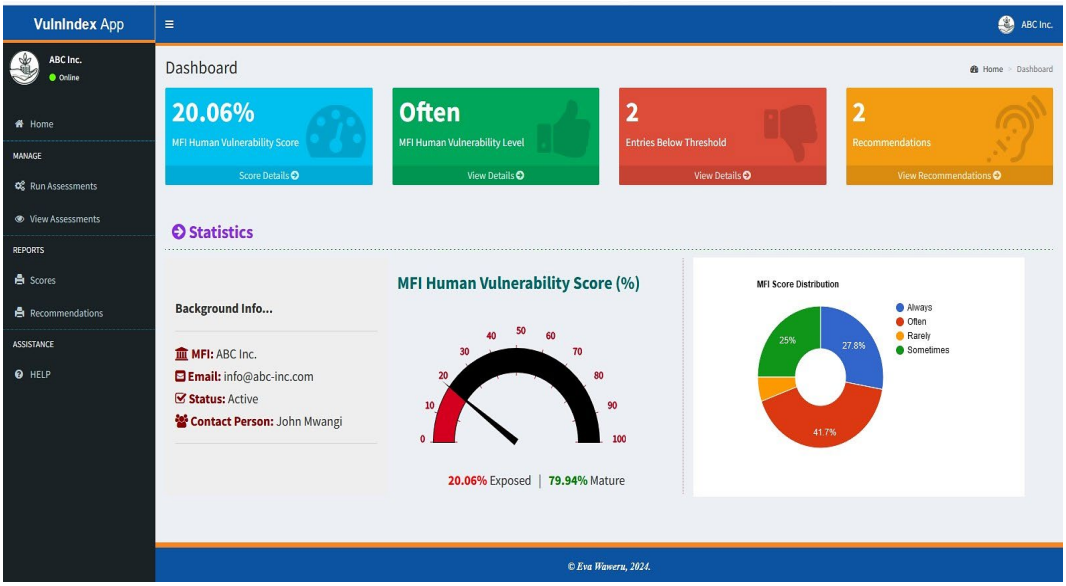


Figure 5. User dashboard.

The system admin is directed to admin dashboard when they are successfully authenticated at the login. The admin dashboard displays such information as the number of MFI users registered, the total number of assessments ran by the MFI users with corresponding scores, the average score computed from all MFI scores posted, the number of questions usable for assessments, and the score distribution chart for all MFI scores. Figure 6 shows the admin dashboard.

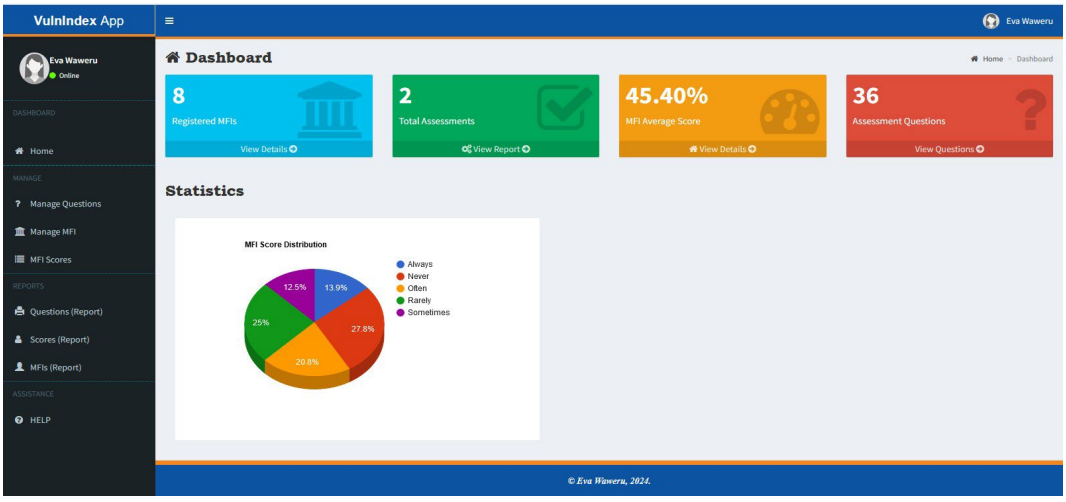
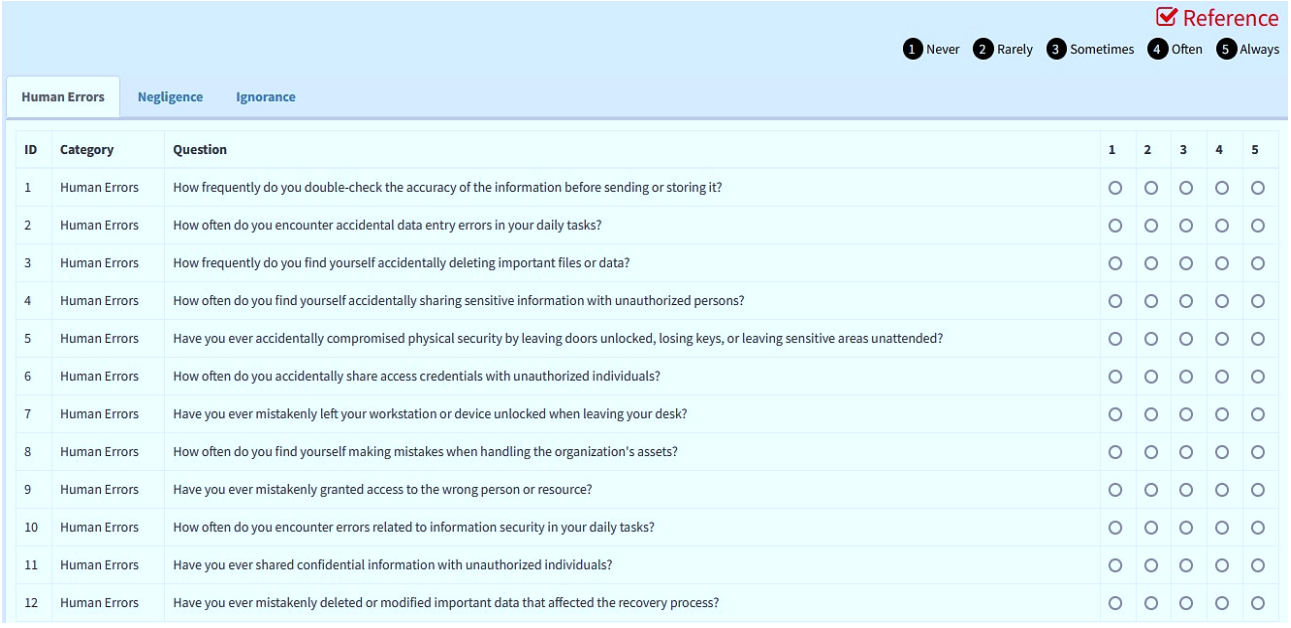


Figure 6. Admin dashboard.

3.1.6. Human Vulnerability Assessment Module

This module enables MFI users to select the best responses to the questions curated for assessment the MFI's human vulnerability index. After that, the user submits the completed form to the database from where computations of the human vulnerability index and its derivatives, including the MFI maturity index will be computed. Figure 7 shows the graphical user interface for the human vulnerability assessment module.



ID	Category	Question	1	2	3	4	5
1	Human Errors	How frequently do you double-check the accuracy of the information before sending or storing it?	○	○	○	○	○
2	Human Errors	How often do you encounter accidental data entry errors in your daily tasks?	○	○	○	○	○
3	Human Errors	How frequently do you find yourself accidentally deleting important files or data?	○	○	○	○	○
4	Human Errors	How often do you find yourself accidentally sharing sensitive information with unauthorized persons?	○	○	○	○	○
5	Human Errors	Have you ever accidentally compromised physical security by leaving doors unlocked, losing keys, or leaving sensitive areas unattended?	○	○	○	○	○
6	Human Errors	How often do you accidentally share access credentials with unauthorized individuals?	○	○	○	○	○
7	Human Errors	Have you ever mistakenly left your workstation or device unlocked when leaving your desk?	○	○	○	○	○
8	Human Errors	How often do you find yourself making mistakes when handling the organization's assets?	○	○	○	○	○
9	Human Errors	Have you ever mistakenly granted access to the wrong person or resource?	○	○	○	○	○
10	Human Errors	How often do you encounter errors related to information security in your daily tasks?	○	○	○	○	○
11	Human Errors	Have you ever shared confidential information with unauthorized individuals?	○	○	○	○	○
12	Human Errors	Have you ever mistakenly deleted or modified important data that affected the recovery process?	○	○	○	○	○

Figure 7. Assessment module.

3.1.7. Human Vulnerability Index Gauge

The formula derived after regression analysis in chapter four was implemented in the model basically to compute the human vulnerability index for MFI. The computation summary is presented in the code snippet in Figure 8 and the human vulnerability and maturity gauge is presented in Figure 9.

$$Y = \alpha + B1X1 + B2X2 + B3X3 + \cdots + BnXn + e$$

$$\text{CSHCEI} = -0.062 + \left(0.167^{*} H.E\right) + \left(0.539^{*} N.G\right) + \left(0.324^{*} I.G\right) + 0.32$$

```php
<?php
    $user = $_SESSION['user'];
    $sql = "SELECT ROUND((-0.062+SUM(b.weight*a.score)+0.32)/(-0.062+SUM
      (b.weight*5)+0.32)*100,2) FROM assessments a inner join questions
      b on a.question_id=b.id where user_id='$user'";
    $result = mysqli_query($conn,$sql);
    $data = mysqli_fetch_array($result);
    $vuln = $data[0];
    if($vuln == 0){
      echo 0;
    }else{
      echo $vuln;
    }
?>
```

Figure 8. Human vulnerability index computation code.

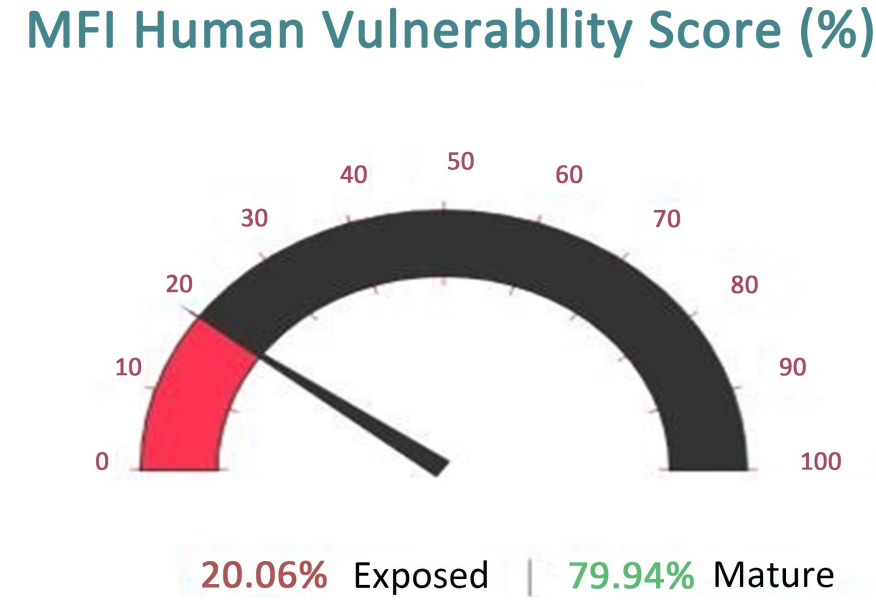


Figure 9. Human vulnerability index gauge.

3.1.8. MFI Score Distribution

The system displays the distribution of scores with respect to five agreement levels to assessment questions, namely: always, often, rarely, and never. This helps the MFI users to know the level of human vulnerability in their organization based on the honest response to human vulnerability questions. The presentation of the score distribution is presented as a pie chart graph shown in Figure 10.

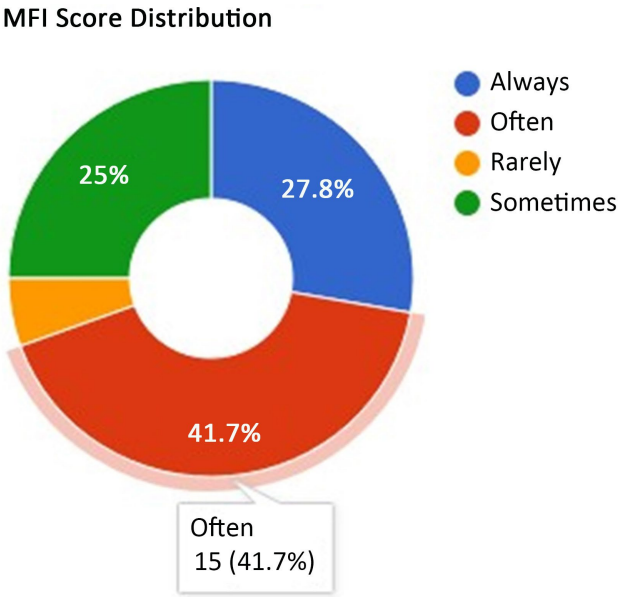
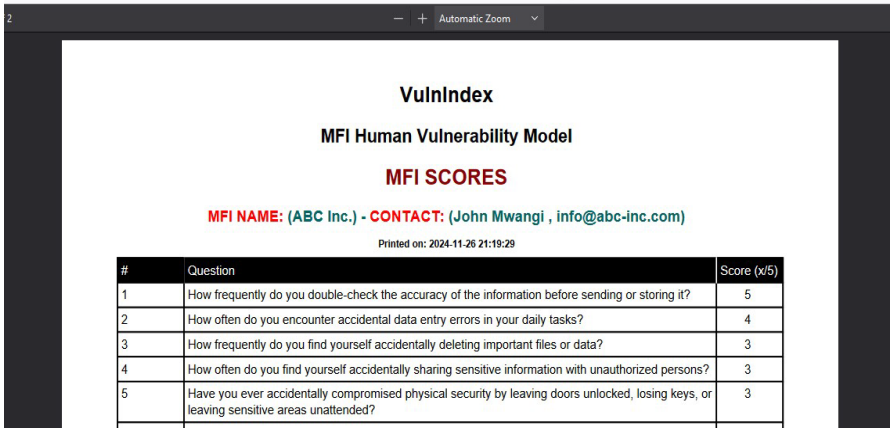


Figure 10. MFI score distribution chart.

3.1.9. System Reports

The user scores report echoes back the values that the user inputs for each assessment question in the course of assessments into a printable report. The MFI rec-

ommendations report generates a list of best practices for each question scored below the threshold. This enables the MFI to have targeted areas in one print that will minimize the human vulnerability and improve the overall security posture of the MFI as illustrated in Figure 11 and Figure 12.



VulnIndex

MFI Human Vulnerability Model

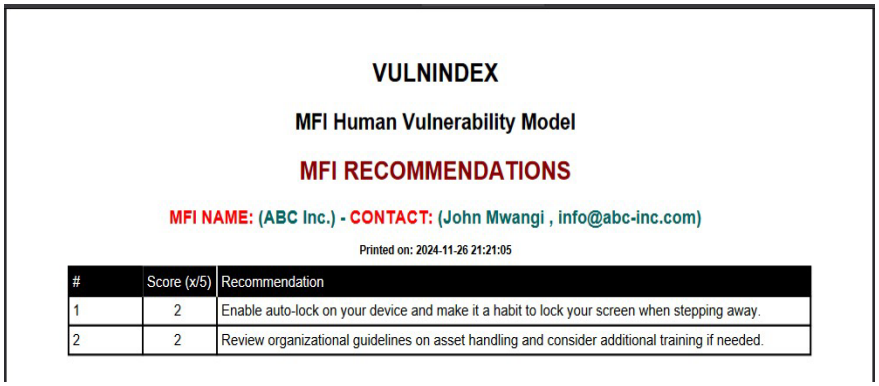
MFI SCORES

MFI NAME: (ABC Inc.) - CONTACT: (John Mwangi , info@abc-inc.com)

Printed on: 2024-11-26 21:19:29

#	Question	Score (x/5)
1	How frequently do you double-check the accuracy of the information before sending or storing it?	5
2	How often do you encounter accidental data entry errors in your daily tasks?	4
3	How frequently do you find yourself accidentally deleting important files or data?	3
4	How often do you find yourself accidentally sharing sensitive information with unauthorized persons?	3
5	Have you ever accidentally compromised physical security by leaving doors unlocked, losing keys, or leaving sensitive areas unattended?	3

Figure 11. MFI user assessment scores report.



VULNINDEX

MFI Human Vulnerability Model

MFI RECOMMENDATIONS

MFI NAME: (ABC Inc.) - CONTACT: (John Mwangi , info@abc-inc.com)

Printed on: 2024-11-26 21:21:05

#	Score (x/5)	Recommendation
1	2	Enable auto-lock on your device and make it a habit to lock your screen when stepping away.
2	2	Review organizational guidelines on asset handling and consider additional training if needed.

Figure 12. MFI recommendation report.

3.1.10. Model Accessibility

The human vulnerability assessment system was developed as a web-based application to demonstrate the practical implementation of the proposed model. To achieve this, a set of robust web development tools was employed: Bootstrap 4 for layout design and styling, jQuery and JavaScript for interactive features and animations particularly within the output panels PHP (Hypertext Preprocessor) as the server-side language for data insertion and retrieval, and MySQL for database management and record storage. The completed system was deployed on a publicly accessible web server and can be accessed remotely.

4. Results

The study examined how human errors, negligence, and ignorance contribute to the Cybersecurity Human Vulnerabilities Exposure Index (CSHVEI) across Microfinance Institutions (MFIs) in Nairobi County. A total of 112 valid responses

were obtained (85% response rate). Reliability tests confirmed strong internal consistency across all constructs (α = 0.935 – 0.957), and multicollinearity diagnostics indicated acceptable VIF values (3.2 - 5.039).

4.1. Descriptive Results

Findings show that MFIs maintain moderate levels of cybersecurity awareness, but significant behavioural vulnerabilities persist.

Human Errors: Accidental deletion of files (43%), data entry mistakes (38%), and inadvertent sharing of sensitive information (46%) were frequently reported.

Negligence: Non-adherence to protocols was prominent, including password sharing (41%), leaving machines unlocked (52%), and bypassing procedures for convenience (55%).

Ignorance: Training gaps were evident; only 45% reported receiving adequate cybersecurity training, and 41% admitted to ignoring or delaying security alerts.

4.2. Spearman Rank Correlation Analysis

The degree and direction of the relationship between two ranked variables are measured by Spearman's correlation coefficient, or ρ, which is also represented by r_s. Table 1 shows the findings of these correlations between independent and dependent variables.

Table 1. Correlations matrix.

			CSHVEI	Human Errors	Negligence	Ignorance
Spearman's rho	Cyber Security Human Exposure Index (CSHVEI)	Correlation Coefficient	1.000			
		Sig. (2-tailed)	.			
		N	112			
	Human Errors	Correlation Coefficient	0.654**	1.000		
		Sig. (2-tailed)	0.000	.		
		N	112	112		
	Negligence	Correlation Coefficient	0.818**	0.601**	1.000	
		Sig. (2-tailed)	0.000	0.000	.	
		N	112	112	112	
	Ignorance	Correlation Coefficient	0.831**	0.668**	0.702**	1.000
		Sig. (2-tailed)	0.000	0.000	0.000	.
		N	112	112	112	112

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

According to the results, there is a statistically significant relationship between human errors and cyber security human exposure index (r^s = 0.654; p = 0.000). Secondly, it was observed that there was evidence of a significant relationship between negligence and cyber security human exposure index (r^s = 0.818; p = 0.000).

Finally, it was evident that ignorance significantly associates with cyber security human exposure index ($r^s = 0.831$; $p = 0.000$).

4.3. Regression Analysis

Regression analysis is a statistical technique that models how changes in one or more independent variables impact a dependent variable. It is therefore a powerful statistical method that allows you to examine the relationship between two or more variables of interest.

4.3.1. Summary Table

This segment indicates the model characteristics including R, R-Square, adjusted r-square and standard error of the estimate (Table 2).

Table 2. Model summary.

Model	R	R Square	Adjusted R Square	Std. Error
1	0.951[a]	0.905	0.902	0.32341

Note: a. Predictors: (Constant), Ignorance, Negligence, Human Errors, b. Dependent Variable: Cyber Security Human Exposure Index (CSHVEI).

The model summary shows that 90.2 % in Cyber Security Human Exposure Index (CSHVEI) can be explained by using the three predictors (ignorance, negligence, human errors). The coefficient of determination in this study is 0.905. This coefficient evaluates the accuracy with which a statistical model predicts the outcome.

4.3.2. ANOVA

When two regression models are compared, the ANOVA function determines whether there is a significant difference between them (Table 3).

Table 3. ANOVA.

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	107.055	3	35.685	341.184	0.000[b]
	Residual	11.296	108	0.105		
	Total	118.351	111			

Note: a. Dependent Variable: Cyber Security Human Exposure Index (CSHVEI), b. Predictors: (Constant), Ignorance, Negligence, Human Errors.

The robustness of this model is assessed using ANOVA. It shows that the model is highly significant in predicting Cyber Security Human Exposure Index (CSHVEI), $F(3,108) = 341.184$, $p < 0.05$, Adjst. R square = 0.902.

4.3.3. Coefficients

In this paper, multiple linear regression was employed. The main objective of mul-

tiple regression is to examine the extent of influence of the independent variable on the dependent variable. Regression coefficients provide the model weights (Table 4).

Table 4. Coefficients.

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	−0.062	0.110		−0.562	0.576		
	Human Errors	0.167	0.061	0.172	2.729	0.007	0.224	4.471
	Negligence	0.539	0.053	0.539	10.128	0.000	0.313	3.200
	Ignorance	0.324	0.072	0.298	4.472	0.000	0.198	5.039

Note: a. Dependent Variable: Cyber Security Human Exposure Index (CSHVEI).

The findings shows that human errors significantly contribute to Cyber Security Human Exposure Index ($\beta = 0.167$; $p < 0.05$). Furthermore, negligence significantly influences Cyber Security Human Exposure Index at 0.05 alpha ($\beta = 0.539$; $p < 0.05$). Finally, it was established that Ignorance significantly affect Cyber Security Human Exposure at 0.05 alpha level ($\beta = 0.324$; $p < 0.05$).

Index Calculation:

$$Y = \alpha + B1X1 + \cdots B2X2 + B3X3 + e$$

$$\text{CSHVEI} = -0.062 + 0.167(\text{Human Errors}) + 0.539(\text{Negligence}) + 0.324(\text{Ignorance})$$

Human Vulnerability Index Calibration:

The model elicits responses from MFI users on a 1 - 5 Likert scale, where 1 denotes *never* and 5 denotes *always*. Consequently, system calibration begins not at zero but at the minimum possible score of 1 across all items. When a user selects 1 for every question, indicating complete non-compliance with the assessment criteria, the model yields an exposure index of 79.67% and a corresponding maturity index of 20.33% (see Figure 13).

Because the scale does not include zero, the lowest attainable maturity score necessarily corresponds to the highest exposure score. Thus, the instrument can validly measure a human vulnerability (maturity) index ranging from 0.2033 to 1, or 20.33% to 100%. Scores below 0.2033 lie outside the model's theoretical range and therefore represent an impossible state.

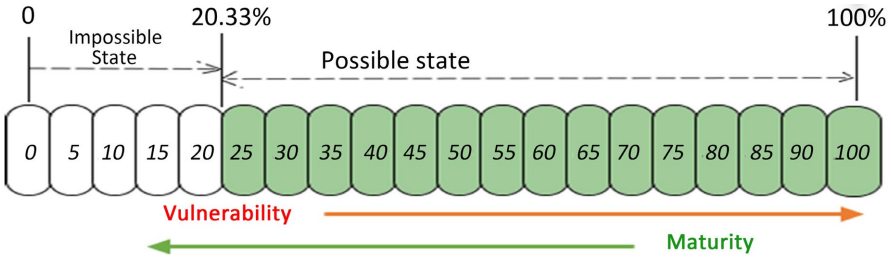


Figure 13. Model cases.

5. Discussion

The findings of this study demonstrate that human-factor vulnerabilities significantly elevate cybersecurity exposure within Microfinance Institutions. Among the three assessed dimensions, negligence emerged as the dominant contributor to cybersecurity exposure, indicating that non-compliance with established security procedures poses a greater risk than lack of knowledge or unintentional mistakes. This suggests that behavioral disregard for controls, rather than their absence, is the most critical driver of human-induced cyber risk in MFIs.

Ignorance also showed a substantial influence on cybersecurity exposure. Gaps in cybersecurity training, inconsistent awareness programs, and delayed responses to security alerts point to deficiencies in institutional learning and reinforcement mechanisms. These findings indicate that awareness initiatives within MFIs are often reactive or fragmented, rather than continuous and embedded within organizational culture. As a result, employees may possess partial knowledge of cybersecurity requirements without fully understanding their practical implications or urgency.

Human errors, while comparatively less influential than negligence and ignorance, remained a statistically significant predictor of cybersecurity exposure. Operational mistakes such as accidental deletion of files, misconfiguration of systems, and mishandling of sensitive information reflect cognitive limitations and workload pressures common in resource-constrained environments. These errors align with global evidence showing that unintentional insider actions remain a persistent source of cyber risk, even in organizations with formal security policies in place.

Collectively, these results reinforce the argument that cybersecurity exposure in MFIs is predominantly socio-technical in nature. Technical controls alone are insufficient when human behavior, awareness, and compliance are misaligned with security objectives. The high explanatory power of the model confirms that human-related factors account for the majority of variation in cybersecurity exposure, underscoring the need to integrate behavioral metrics into cybersecurity risk management frameworks.

A key contribution of this study lies in the development and validation of the Cybersecurity Human Vulnerabilities Exposure Index. Unlike existing frameworks that acknowledge human factors without providing quantifiable assessment mechanisms, the CSHVEI translates human behavior and organizational practices into measurable exposure components. By consolidating diverse human-related controls into the three domains of human error, ignorance, and negligence, the model offers a structured and analytically manageable approach for assessing human-centric cybersecurity risk.

The empirical weighting of the vulnerability domains yields important practical insights. The predominance of negligence challenges the common assumption that cybersecurity incidents are primarily the result of accidental mistakes. Instead, persistent procedural non-compliance and convenience-driven behavior emerge as

the most significant contributors to exposure. This finding suggests that organizations may achieve greater risk reduction by strengthening enforcement, accountability, and behavioral incentives, rather than focusing exclusively on awareness training.

The prototype implementation further demonstrates the practical applicability of the CSHVEI. Its modular architecture, incorporating posture assessment, automated computation, score visualization, and targeted recommendations, enables organizations to move from abstract risk recognition to actionable intervention. The system allows MFIs to identify specific vulnerability hotspots and prioritize mitigation measures such as policy reinforcement, access control adjustments, and continuous training programs.

The calibration results provide additional insight into organizational risk dynamics. Even minimal non-compliance produced relatively high exposure scores, indicating that human-related cybersecurity risk accumulates rapidly. This underscores the importance of continuous behavioral vigilance and institutional reinforcement, rather than one-off training sessions or periodic audits. Cyber attackers increasingly exploit routine behavior, trust, and procedural shortcuts, making sustained compliance a critical component of cybersecurity resilience.

Overall, the findings confirm that human behavior represents a central determinant of cybersecurity exposure within MFIs. The CSHVEI offers a practical, evidence-based tool for quantifying this exposure and supporting informed decision-making. By integrating human-factor metrics into cybersecurity governance, organizations can better prioritize interventions, monitor behavioral maturity, and reduce their attack surface. While further validation across additional sectors is recommended, the model establishes a robust foundation for embedding human-centric assessment into broader cybersecurity risk management strategies.

6. Conclusions

This study set out to address the persistent gap in cybersecurity research and practice concerning the systematic assessment of human-induced vulnerabilities. While cybersecurity frameworks commonly acknowledge the importance of people alongside processes and technology, they offer limited mechanisms for quantifying how human behavior contributes to organizational cyber exposure. In response to this gap, the study developed and validated the Cybersecurity Human Vulnerabilities Exposure Index (CSHVEI) as a practical and evidence-based tool for measuring human-related cybersecurity risks within Microfinance Institutions.

The findings confirm that human factors play a dominant role in shaping cybersecurity exposure. Negligence emerged as the most influential contributor, followed by ignorance and human error, demonstrating that procedural non-compliance and behavioral disregard for controls pose greater risks than accidental mistakes alone. These results highlight the need for organizations to move beyond technology-focused security strategies and adopt approaches that actively address

behavior, accountability, and security culture.

By translating human behavior into measurable exposure components, the CSHVEI provides organizations with a structured method to assess, compare, and monitor human-centric cybersecurity risks. The prototype implementation further illustrates the operational viability of the model, enabling institutions to identify vulnerability hotspots, prioritize interventions, and evaluate improvements over time. This positions the CSHVEI as both an analytical framework and a practical decision-support tool for cybersecurity governance.

The study contributes to cybersecurity literature by empirically demonstrating the socio-technical nature of cyber risk and by offering a quantifiable model that complements existing standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework. For practitioners and policymakers, the model offers a scalable approach to strengthening cybersecurity resilience, particularly in resource-constrained environments.

Future research should extend the validation of the CSHVEI across other sectors and geographic contexts and explore the integration of real-time data analytics and machine learning techniques to enhance predictive capability. Such extensions would further strengthen the model's applicability and support the development of adaptive, human-centered cybersecurity risk management strategies.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Too, W.K. and Kibet, A. (2025) The Defensive Cyber Security Readiness Model for Higher Education. *International Journal of Innovative Science and Research Technology*, **10**, 1763-1771. https://doi.org/10.38124/ijisrt/25mar1158

[2] Hughes-Lartey, K., Li, M., Botchey, F.E. and Qin, Z. (2021) Human Factor, a Critical Weak Point in the Information Security of an Organization's Internet of Things. *Heliyon*, **7**, e06522. https://doi.org/10.1016/j.heliyon.2021.e06522

[3] Liu, X., Ahmad, S.F., Anser, M.K., Ke, J., Irshad, M., Ul-Haq, J., *et al.* (2022) Cyber Security Threats: A Never-Ending Challenge for E-Commerce. *Frontiers in Psychology*, **13**, Article ID: 927398. https://doi.org/10.3389/fpsyg.2022.927398

[4] Ertan, A., Floyd, K., Pernik, P. and Stevens, T. (2021) Cyber Threats and NATO 2030: Horizon Scanning and Analysis. CCDCOE.

[5] Kibet, A. (2025) Enhancing Transparency and Security in Means Testing for Education Financing: A Blockchain-Based Approach. 2025 *IST-Africa Conference* (*IST-Africa*), Nairobi, 28-30 May 2025, 1-14. https://doi.org/10.23919/ist-africa67297.2025.11060559

[6] Kaur, J. and Ramkumar, K.R. (2022) The Recent Trends in Cyber Security: A Review. *Journal of King Saud University-Computer and Information Sciences*, **34**, 5766-5781. https://doi.org/10.1016/j.jksuci.2021.01.018

[7] 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

[8] Hadrian (2023) Assessing from the Outside in. Hadrian.

[9] Grassegger, T. and Nedbal, D. (2021) The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering. *Procedia Computer Science*, **181**, 59-66. https://doi.org/10.1016/j.procs.2021.01.103

[10] Kibet, A. (2026) A Design Science Study of Blockchain-Based Governance and Incentive Architectures for Ride-Sharing Platforms. *Open Journal of Applied Sciences*, **16**, 300-319. https://doi.org/10.4236/ojapps.2026.161019

[11] Kibet, A., Thiga, M.M. and Karume, S.M. (2019) Towards a Blockchain Based Smart Contracts Model Design for Housing Market Applications. *International Journal of Advanced Research in Computer Engineering & Technology* (*IJARCET*), **8**, 327-334.

[12] Kibet, A. and Karume, S.M. (2018) A Synopsis of Blockchain Technology. *International Journal of Advanced Research in Computer Engineering & Technology* (*IJARCET*), **7**, 789-795.

[13] Dai, K., Kawaki, I.L. and Sakti, L.D. (2023) Mitigation of Cyber Security Risk Threats during the COVID-19 Pandemic. *International Journal of Cyber and IT Service Management*, **3**, 107-119. https://doi.org/10.34306/ijcitsm.v3i2.135

[14] Kibet, A. (2019) Designing a Blockchain Based Smart Contract Model: A Case of Real Estate Industry. *International Journal of Advanced Research in Computer Engineering & Technology* (*IJARCET*), **8**.

[15] Nobles, C. (2022) Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem. *HOLISTICA—Journal of Business and Public Administration*, **13**, 49-72. https://doi.org/10.2478/hjbpa-2022-0003

[16] Nifakos, S., Chandramouli, K., Nikolaou, C.K., *et al.* (2021) Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. *Sensors*, **21**, 5119. https://doi.org/10.3390/s21155119

[17] Hadlington, L. (2020) The "Human Factor" in Cybersecurity. In: Information Resources Management Association, Ed., *Research Anthology on Artificial Intelligence Applications in Security*, IGI Global, 1960-1977. https://doi.org/10.4018/978-1-7998-7705-9.ch087

[18] Communications Authority of Kenya (CA) (2025) Cybersecurity Report. Communications Authority of Kenya (CA).

[19] Wang, Z., Zhu, H. and Sun, L. (2021) Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. *IEEE Access*, **9**, 11895-11910. https://doi.org/10.1109/access.2021.3051633

[20] Georgiadou, A., Mouzakitis, S. and Askounis, D. (2022) Detecting Insider Threat via a Cyber-Security Culture Framework. *Journal of Computer Information Systems*, **62**, 706-716. https://doi.org/10.1080/08874417.2021.1903367

[21] Suryotrisongko, H. and Musashi, Y. (2019) Review of Cybersecurity Research Topics, Taxonomy and Challenges: Interdisciplinary Perspective. 2019 *IEEE* 12*th Conference on Service-Oriented Computing and Applications* (*SOCA*), Kaohsiung, 18-21 November 2019, 162-167. https://doi.org/10.1109/soca.2019.00031

[22] Onwubiko, C. and Ouazzane, K. (2022) Multidimensional Cybersecurity Framework for Strategic Foresight. *International Journal on Cyber Situational Awareness*, **6**, 46-77. https://doi.org/10.22619/ijcsa.2021.100137

[23] Dash, B. and Ansari, M.F. (2022) An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy. *International Research Journal of Engineering and Technology* (*IRJET*), **9**, 1-6.

[24] Zimmermann, V. and Renaud, K. (2019) Moving from a 'Human-as-Problem" to a 'Human-as-Solution" Cybersecurity Mindset. *International Journal of Human-Computer Studies*, **131**, 169-187. https://doi.org/10.1016/j.ijhcs.2019.05.005

[25] Sundar, S.S. and Kim, J. (2019) Machine Heuristic: When We Trust Computers More than Humans with Our Personal Information. *Proceedings of the* 2019 *CHI Conference on Human Factors in Computing Systems*, Scotland, 4-9 May 2019, 1-9. https://doi.org/10.1145/3290605.3300768

[26] Mazzarolo, G. and Jurcut, A.D. (2019) Insider threats in Cyber Security: The Enemy within the Gates. Cornell University.

[27] Greitzer, F.L. (2019) Insider Threats: It's the Human, Stupid! *Proceedings of the Northwest Cybersecurity Symposium*, Richland, 8-10 April 2019, 1-8. https://doi.org/10.1145/3332448.3332458

[28] Lee, I. (2022) Analysis of Insider Threats in the Healthcare Industry: A Text Mining Approach. *Information*, **13**, Article 404. https://doi.org/10.3390/info13090404

[29] Ahsan, M., Nygard, K.E., Gomes, R., Chowdhury, M.M., Rifat, N. and Connolly, J.F. (2022) Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review. *Journal of Cybersecurity and Privacy*, **2**, 527-555. https://doi.org/10.3390/jcp2030027

[30] Alghamdi, M.I. (2021) History, Present 2021 and Future of Cyber Attacks. *Journal of Cybersecurity and Information Management*, **8**, 71-83. https://doi.org/10.54216/jcim.080204

[31] Ulven, J.B. and Wangen, G. (2021) A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet*, **13**, Article 39. https://doi.org/10.3390/fi13020039

[32] Prabhu, S. and Thompson, N. (2022) A Primer on Insider Threats in Cybersecurity. *Information Security Journal: A Global Perspective*, **31**, 602-611. https://doi.org/10.1080/19393555.2021.1971802

[33] Solove, D.J. and Hartzog, W. (2022) Breached! Why Data Security Law Fails and How to Improve It. Oxford University Press.

[34] Papatsaroucha, D., Nikoloudakis, Y., Kefaloukos, I., Pallis, E. and Markakis, E.K. (2021) A Survey on Human and Personality Vulnerability Assessment in Cybersecurity: Challenges, Approaches, and Open Issues. arXiv:2106.09986.