A MODEL TO DETERMINE CYBER SECURITY HUMAN VULNERABILITIES EXPOSURE INDEX FOR MFIs
(A CASE STUDY OF NAIROBI COUNTY, KENYA)

EVALINE NJERI WAWERU

A THESIS SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY IN THE SCHOOL OF COMPUTING AND MATHEMATICS IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF SCIENCE IN CYBER SECURITY OF THE CO-OPERATIVE UNIVERSITY OF KENYA

2025

DECLARATION

I declare that this thesis is my original work and has not been presented for award of a degree in any other university or for any other award.

Signature …… Date …….4th Feb 2025.....

Evaline Waweru

MCSC01/6013/2022

Declaration by the supervisors

We confirm that the work reported in this thesis was carried out by the candidate under our supervision and has been submitted with our approval as university supervisors

Signature …… Date …….4th Feb 2025.....

Prof. Simon Maina Karume

Department of Computing and Informatics,

The Cooperative University of Kenya

Signature …… Date ……4th Feb 2025….....

Dr. Alex Kibet

Department of Computing and Informatics,

Laikipia University

DEDICATION

I dedicate this degree to my kids, brothers and cousins as a testament that through hard work and dedication, dreams can become a reality.

ACKNOWLEDGEMENTS

I owe it all to God for this significant milestone in life. I am grateful for the blessings, knowledge, sound mind, opportunities, and resources bestowed upon me.

First and foremost, I am deeply grateful to my supervisor, Prof. Karume and Dr. Alex for their invaluable guidance throughout the entire duration of this project. I count it a blessing from above. I would like to extend my heartfelt thanks to the faculty members of the institute particularly Prof.Kihoro for pushing and encouraging me towards pursuing my master's degree. Dr. Shem, Dr. Katila, Dr. Omollo, Dr. Mile, Dr. Fidelis and Dr. Muriuki for their mentorship and intellectual contributions.

I am also indebted to my coursemates who have offered support and insightful discussions towards this big milestone. Special thanks to my dear husband Zack who has been my pillar of support from the very beginning. To all my family members who have played a role in shaping me into the person I am today, I am immensely grateful.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURE

LIST OF ABBREVIATIONS

CS	Cyber Security
HF	Human factors
HFVI	Human Factors Vulnerability Index
CSHVEI	Cyber Security Human Vulnerability Exposure Index
NIST	National institute of standards and Technology
COBIT	Control Objectives for information and related technologies
ISO	International organization for standardization
MCDA's	Ministries, Counties, Departments, and government agencies
IoT	Internet of Things
DOS	Denial of Service
MFIs	Micro Finance Institutions

Table 1: CONCEPTUAL AND OPERATIONAL DEFINITION OF TERMS

Cybersecurity Exposure Index	From 0 to 1, CEI calculates the level of exposure to cybercrime by country. The higher the score the higher the higher the exposure
Cybersecurity Framework	Set of documents describing guidelines, standards, and best practices designed for cyber security risk management
Human Factors	Refers to the situations when human errors result in a successful data or security breach
Cyber security Model	It's a framework used by an organization to measure an organization's level of maturity and ability to identify cybersecurity threats and risks and to guide the selection of policies, strategies, and programs to defend against threats and mitigate risks
Attack Surface	It refers to the number of all possible points, or attack vectors where an unauthorized user can access a system and extract data
Cyber Security	It is the process of ensuring the security of cyberspace from known to unknown threats
Web-based application	An application program that is stored on a remote server and delivered over the internet through a browser interface
Operational Security	Operational Security refers to a systematic approach used to identify, analyse, and protect sensitive information that could be used by attackers to compromise the confidentiality, integrity, and availability of the overall operation of an organization. It involves assessing the organization's activities,
	procedures, and information flows from the perspective of potential adversaries. This helps to identify vulnerabilities and potential attack vectors that could be exploited. The goal is to manage and control the release of information to ensure that sensitive data and critical operations are protected.

ABSTRACT

This study developed a model to determine the Cyber Security Human Vulnerability Exposure Index (CSHVEI) for Microfinance Institutions (MFIs) in Nairobi County, Kenya. While people are a critical component of organizational security, they often represent the most significant vulnerability. An integrative literature review identified key human factor vulnerabilities, which were consolidated into three core variables: human error, negligence, and ignorance. A survey was administered to 132 respondents from 52 MFIs, achieving an 85% response rate (n=112). The collected data was analyzed using Spearman's rank correlation and multiple linear regression. The regression analysis produced a highly significant model ($F(3,108) = 341.184$, $p < .05$) that explained 90.2% of the variance in the CSHVEI (Adjusted $R^2 = .902$). The resulting formula, CSHVEI = -0.062 + (0.167 × Human Error) + (0.539 × Negligence) + (0.324 × Ignorance), was implemented and validated via a web-based prototype. The study concludes that negligence is the most weighted factor influencing human vulnerability. The model provides MFIs with a tool to quantify their human factor exposure, enabling targeted interventions to strengthen their overall cybersecurity posture.

Key Words: *human factors, MFIs, cyber security, exposure index, model, negligence*

CHAPTER ONE

1. INTRODUCTION

1.0 Introduction

This Chapter provided a background of the fundamental concepts including the problem informing the proposed study and the justification for the necessity to provide CSHVEI in organizations. It further outlined the research objectives, listed the research questions, defined the scope, assumptions, and the significance of the study

1.1 Background of the Study

The rapid expansion of cyberspace has created both significant opportunities and complex challenges, particularly in the domain of cybersecurity. Security breaches involving sensitive information—especially personal data—have become increasingly common in recent years, as observed by Lartey (2021). Understanding the human element in cyber-attacks is critical. Liu et al. (2022) emphasize that the success of cyber-attacks often depends on the attackers' ability to access and manipulate information during an intrusion. Consequently, safeguarding computing assets and ensuring the confidentiality, integrity, and availability of data have become central components of modern cybersecurity strategies.

As global digital transformation accelerates, cybersecurity threats have grown at an unprecedented rate. Kaspersky (2023) reports that more than 80% of breaches involve human elements such as negligence, ignorance, or human error. Financial institutions are particularly attractive targets because they handle high-value data (IBM Security, 2022). Regionally, Africa has recorded a threefold increase in social-engineering attacks over the past five years (AUDA-NEPAD, 2022). In Kenya, the Communications Authority (2023) notes that approximately 70% of cyber incidents stem from human-related weaknesses, including phishing, compromised credentials, and insider misuse. Microfinance institutions (MFIs), in particular, face heightened exposure due to limited cybersecurity budgets and inadequate staff training (FSD Kenya, 2021).

Education and awareness have become essential as cyber threats evolve. Sairi et al. (2020) emphasize the importance of educating new generations about cybersecurity concepts. Negligence and insufficient awareness remain dominant contributors to cyber-crime, as highlighted by Kaur and Ram Kumar (2022). The escalation of cyber threats therefore demands

proactive measures to protect systems, infrastructure, and information assets from malicious activities (Ertan et al., 2020).

Despite advancements in technology, many organizations remain highly vulnerable. Kaur and Ram Kumar (2022) report that 83% of retailers in the United States were at risk of cyber-attacks. E-commerce organizations and customers continue to be key targets for cybercriminals seeking to steal private information (D'Adamo et al., 2021). Attackers utilize diverse methods—including database breaches, malware, ransomware, e-skimming, distributed denial-of-service attacks, and phishing—to exploit security gaps. The rapid expansion of e-business and e-commerce has created new opportunities but simultaneously broadened the cybersecurity challenge (Hadrian, 2023).

Hadrian (2023) defines attack surfaces as the collective digital, physical, and human assets that can be exploited for unauthorized access. While physical and digital attack surfaces are widely recognized, the human attack surface poses particularly severe risks. Employee behaviors—whether intentional or accidental—introduce vulnerabilities that significantly elevate security risks.

Human error, negligence, and lack of awareness make individuals the weakest link in organizational cybersecurity. Numerous studies show that a majority of data breaches result from human-enabled errors such as clicking malicious links, using unsecured Wi-Fi, or sharing confidential information through social media (Hadrian, 2023). The healthcare sector exemplifies the magnitude of this challenge: 93% of security breaches have been attributed to human error and cultural factors, resulting in over 150 million patient records being compromised between 2009 and 2014 in the United States. The shift to digital patient records provided fertile ground for attackers to execute systematic attacks (Nifakos et al., 2021).

Cybercriminals increasingly target human vulnerabilities rather than machine weaknesses. Papatsaroucha et al. (2021) note that factors such as trust, willingness to help, and individual social or cultural characteristics influence susceptibility to deception. Despite their significance, human factors remain underexplored in information security literature (Nobles, 2022). Organizations invest heavily in technology, yet attackers continue to exploit human vulnerabilities to infiltrate networks, systems, and data. Nobles (2022) reports that Symantec identified over 401 million new malware variants in 2016 alone, demonstrating the pace at which attackers exploit emerging technologies, especially Internet of Things devices. While

many organizations prioritize technical controls, behavioral-based risks are often insufficiently addressed (Liu et al., 2022).

1.2 The Problem Statement

The fundamental components of a cyber-secure and resilient organization encompass people, processes, and technology. However, the existing body of research predominantly concentrates on technology and processes, often overlooking the critical aspect of people, which can serve as a vulnerable point of attack. according to Rahman et al., (2021), humans are often considered to be the weakest link in the cyber-security chain.

The rapid growth of cyberspace and the increasing prevalence of cyber threats have highlighted the critical need for effective cybersecurity measures in organizations. Despite the implementation of technological solutions, organizations continue to face vulnerabilities due to the human factor in cybersecurity (Hughes-Lartey et al., 2021). Human error, negligence, and lack of awareness contribute significantly to data breaches and cyber incidents. Existing cybersecurity frameworks often overlook comprehensive approaches to evaluate the effectiveness of security awareness training, user behavior, and the impact of social engineering attacks.

Furthermore, the evolution of cyber threats and the expansion of business technologies, including e-business and e-commerce, have created challenges for organizations, particularly regarding cyber security. Attackers target e-commerce entities and customers, employing various tactics such as data theft, malware, ransomware, and distributed denial of service attacks. Additionally, the human attack surface, encompassing employee behaviours and weaknesses, introduces significant risks to organizational security. (Liu et al., 2022)

Locally, organizations struggle with cybersecurity incidents, and insufficient training and the lack of mandated policies and infrastructure in public universities exacerbate the problem. The existing cybersecurity frameworks, while addressing human factors to some extent, fall short in providing comprehensive assessments of security awareness, user behaviour, and social engineering impacts. (Sairi et al., 2020) Therefore, the problem that was addressed in this study was the lack of a comprehensive model to effectively determine and quantify the Cyber Security Human Factor Exposure Index (HFEI) for organizations

1.3 Objectives of the Study

1.3.1 General Objective of the Study

The main objective of this study was to develop a model that would help in determining the Cyber Security Human Vulnerabilities Exposure Index in MFIs

1.3.2 Specific Objectives of the Study

(i) To determine cyber security human factor vulnerabilities in MFIs

(ii) To derive the cyber security human factor exposure index model for MFIs

(iii) To implement the cyber security human factor exposure index model for MFIs

(iv) To validate the model for cyber-security human factor exposure index

1.4 Research Questions

The researcher sought to find answers to the following questions.

(i) What is the cyber security human factor vulnerabilities in cyber security?

(ii) How can a cyber-security human factor exposure index model in MFIs be derived?

(iii) How can a cyber-security human factor exposure index model be implemented?

(iv) How can the implemented model be verified and validated?

1.5 Expected outcomes of the study

This research study sought to develop a model that would provide the following deliverables: a report on cyber security human factors vulnerabilities in MFIs, a derived cyber security human factor exposure index model, a model that would determine cyber security human factor exposure index, and a verified and validated model report on determining cyber security human factor exposure index

1.6 Justification of the study

The exponential growth in the use of cyberspace has been shadowed by a proportional increase in cyber-attacks, leading to profound negative outcomes including devastating financial losses, operational disruption, and irreparable reputational damage. A vast majority of these breaches are not due to failures in technology, but are propagated through human-related vulnerabilities, making the human element the most significant, yet least managed, risk factor.

While several frameworks exist to guide cybersecurity efforts—such as the NIST CSF, ISO 27001, and others reviewed in this study—they possess a critical weakness: they do not provide a specific, quantitative metric for human factor exposure. They offer qualitative controls and best practices but lack the ability to calculate a definitive Human Vulnerability Exposure Index. This gap leaves organizations, especially resource-constrained MFIs, unable to answer a fundamental question: "How exposed are we, quantitatively, to human-factor risks, and where should we focus our limited resources?"

Hence, the need for a better, more targeted solution is clear. This research is justified by the urgent requirement to move from generic guidance to precise measurement. The proposed CSHVEI model addresses the weaknesses of prior models by providing a quantifiable index

derived from empirical data, enabling Kenyan MFIs to efficiently identify, prioritize, and mitigate the human vulnerabilities that are most aggressively being exploited in today's threat landscape. This directly supports national cybersecurity resilience by strengthening a critical part of the financial sector.

1.7 Scope of the study

This study aimed to develop a model to determine the cyber security human factor exposure index in MFIs. The study was conducted within micro finance institutions operating in Nairobi, Kenya. Focusing on MFIs and Nairobi County provided a relevant context for studying cybersecurity human vulnerabilities. MFIs are critical to financial inclusion yet vulnerable due to resource constraints. Unlike larger financial institutions, MFIs often have limited resources to invest in robust cybersecurity measures. This makes them more vulnerable to human errors, negligence, and ignorance when it comes to handling cybersecurity threats.

Nairobi County, as the financial epicentre, offered a robust case with a high concentration of MFIs exposed to digital risks as compared to other regions in Kenya., making it an ideal location to develop and validate a model for cybersecurity human vulnerability exposure. There was already attempts to measure exposure which this research does not aim at overlap but to improve. This study developed a model supported by a prototype that computed the cyber security human factor exposure index.

1.8 Limitations of the study

The determination of human factor vulnerability was subjective and varied depending on the criteria and indicators used in the study. Different MFIs may have different interpretations and definitions of what constitutes human factor exposure which can lead to discrepancies in the results.

1.9 Significance of the Study

This research is critically justified by the urgent need to address the human factor as the most overlooked yet significant vulnerability in cybersecurity, particularly within Kenya's Microfinance Institutions (MFIs). It directly supports Kenya's national cybersecurity agenda, including the Computer Misuse and Cybercrimes Act, 2018 and the National Cybersecurity Strategy, by providing a practical model to quantify human risk. By enabling MFIs to measure and mitigate human vulnerabilities like negligence and ignorance, the study moves beyond a purely technological defense approach, helping to build a more resilient financial sector and strengthen the nation's critical information infrastructure as mandated by national policy.

1.10 Conclusion

The projected model was built upon the various insights that had been undertaken by various researchers in the business and information technology field to bridge the gap that organizations have been having of overlooking human factors as a key cause of security breaches and would rather prioritize their resources on technological controls and solutions.

CHAPTER TWO

2. LITERATURE REVIEW

2.1 Introduction

This chapter reviewed cyber security and its elements, attack surfaces, the human factors in cybersecurity, the role of human factors in organizations and the importance of addressing human factors in cyber security risk assessment, types of human factors vulnerabilities. It further addressed cyber security building blocks as well as the human factor exposure index and best practices to mitigate the vulnerability risks

2.2 The Pivotal Role of Human Factors in Cybersecurity

Contemporary cybersecurity challenges have fundamentally shifted from purely technical vulnerabilities to complex human-technical interactions. While traditional security models emphasized technological protections for confidentiality, integrity, and availability (CIA triad), evidence consistently demonstrates that human elements constitute both the primary defense mechanism and the most exploited attack vector (Hadlington, 2021). This paradigm shift recognizes that organizational security is ultimately a socio-technical system where human behavior significantly influences security outcomes.

The financial sector exemplifies this vulnerability, particularly microfinance institutions that balance expansive digital services with limited security resources. According to the 2023 Kenya Cybersecurity Report, the financial sector experienced a 47% increase in social engineering attacks, with phishing campaigns specifically targeting employees in financial roles (Communications Authority of Kenya, 2023). This trend reflects global patterns where attackers increasingly bypass technical controls by exploiting human psychology through carefully crafted social engineering tactics (Wang et al., 2021). The success of these approaches stems from their ability to manipulate fundamental human traits including trust, authority response, and urgency perception, making even security-aware employees vulnerable to sophisticated attacks.

Within organizations, human vulnerability manifests through three primary channels: knowledge gaps in security awareness, motivational failures in protocol adherence, and unavoidable cognitive errors. Georgiadou et al. (2022) demonstrated that unintentional insider threats—those resulting from employee mistakes or negligence—account for approximately 68% of security incidents in resource-constrained organizations. This aligns with findings from the 2023 Verizon Data Breach Investigations Report, which identified the human element as a critical factor in 74% of all breaches, primarily through stolen credentials, phishing, and business email compromise. These patterns underscore the urgent need for specialized

assessment tools that can quantify human vulnerability specifically within the financial sector context.

2.3 Cyber Security

According to (Kaspersky, 2023), Cyber security encompasses the proactive measures taken to safeguard computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. Disregarding the importance of cybersecurity is not an option, as a single security breach has the potential to expose the personal information of countless individuals. This, in turn, can trigger severe financial repercussions for companies and erode the trust of their customers and other business/ organizational interested parties.

Consequently, cybersecurity emerged as an indispensable element in shielding both individuals and corporations from the clutches of cybercriminals. At its core, the security of any organization was anchored in three fundamental principles: confidentiality, integrity, and availability, as highlighted by Karin (2023). These principles collectively form the cornerstone of an organization's cybersecurity strategy, working in unison to establish robust and resilient protection against the constantly evolving landscape of cyber threats.

Confidentiality was concerned with controlling access to critical data and preventing any unauthorized disclosure(Atlam, 2020). Its primary goal was to maintain the privacy of an organization's or an individual's data, ensuring that only individuals with appropriate authorization can access it. Atlam (2020) also indicates that integrity pertains to data that was complete, trustworthy, and had not been modified or accidentally altered by an unauthorized user.

Any data that had been subject to tampering or compromise, in essence, forfeited its integrity. While availability ensured that authorized users can get timely and reliable access to the necessary resources whenever they need to. Applications, systems, or data are of no use to an organization or its customers if they are not accessible as and when required (Bandari, 2023)

Figure 1. 1: **CIA Triads of Information Security Source:(Team, 2021)**

2.3.1 Elements of Cyber security

Cyber security elements represent essential areas of an organization's infrastructure necessary for protection from cyber threats (swarnavo, 2022). These include the following;

a) **Network security**

Network security refers to the process of protecting the physical network and the connected devices (Pramanik et al., 2022). According to (Zhang, 2021), Network security involves protecting computer networks and their components from potential threats like disruptive elements such as malware and hacking attempts. It also encompasses various tools, technologies, and practices aimed at maintaining the confidentiality, integrity, and availability of network resources and data. Organizations can prevent unauthorized access, data breaches, and other cyber threats posed by attackers, hackers, and malicious software by employing effective network security measures. According to (Whitman & Mattord, 2021), Some of the ways to enhance network security include;

Use of firewalls: They act as barriers between trusted networks and untrusted networks. It mainly inspects incoming and outgoing traffic using a set of predefined security rules and policies to identify and block threats. An installed and well-configured firewall prevents unauthorized access, protects against various types of cyber threats, and blocks potentially malicious traffic

Securing wireless networks: It is crucial since they are more vulnerable to attacks due to their intrinsic nature of broadcasting signals. Some steps to enhance wireless network security are encryption, SSID Hiding (Service set identifier), MAC addressing filtering, and the use of strong passwords.

Remote Connections and Encryption: This is done by ensuring that remote connections are established through encrypted methods. This is typically achieved using protocols like SSH (Secure Shell) for remote administration and VPNs (Virtual Private Networks) for creating secure encrypted tunnels for remote access.

Intrusion Detection and Prevention Systems (IDPS): These systems monitor network traffic for suspicious activities or patterns that might indicate an ongoing cyberattack. They can detect and respond to various types of attacks in real time, providing an additional layer of security.

Keep a watch on unusual network traffic: Network monitoring to ensure that traffic is within normal range and always investigate any abnormal behavior. More so, tacking interzone communication.

Be cautious of free drives (USB Drop attack): Gifts come at a great cost therefore it's important to be cautious since once these drives are inserted into a computer, they might contain malicious software (malware) designed to exploit vulnerabilities, collect sensitive information like passwords, or create a backdoor for remote access by the attacker. This attack takes advantage of human curiosity or the desire to get something for free, making it an effective social engineering technique.

b) **Application Security**

Application security focuses on protecting software applications from various threats and vulnerabilities that could potentially compromise their confidentiality, integrity, and availability. It involves implementing measures and practices to ensure that the software applications developed or used are robust and resilient against security threats. This includes both web and mobile applications, as well as desktop software (Alkatheiri et al., 2021)

The use of hardware and software such as anti-virus programs, encryption, and firewalls protects the system against threats that may interfere with application development (Alkatheiri et al., 2021). The goal was to identify, mitigate, and prevent vulnerabilities that attackers could exploit to gain unauthorized access, steal data, disrupt services, or otherwise compromise the application's functionality. As defined by (NamLabs Technologies, 2021) some key aspects of application security include:

i. **Authentication**

Authentication was a key security component in applications that confirmed that the user is who he/she is claiming to be. It confirmed the identity of users attempting to log in by verifying the credentials they provide. This can be enhanced by the use of either single-factor authentication or multi-factor authentication. Single-factor authentication (SFA) involves using a single method to verify a user's identity. (Krishnasamy & Venkatachalam, 2023). The most common example is using a username and password combination. Users enter their credentials, and the application checks if they match the stored data. This method can be vulnerable if passwords are weak or compromised.

Multi-factor authentication (MFA) is another more secure method. It adds an extra layer of security by requiring users to provide multiple forms of verification (Tolba & Al-Makhadmeh, 2021). This makes it more challenging for attackers to gain unauthorized access even if they obtain one factor.

ii. **Authorization**

Authorization comes after authentication since the user has to provide their credentials first, then the application validates these credentials to ensure the user's identity. Once the user's identity has been verified, the system checks their permissions to determine whether they have the necessary rights to perform specific actions or access certain parts of the application and its resources. The order of authentication before authorization is crucial for security. If authorization were attempted before authentication, unauthorized users could potentially access resources or actions they shouldn't have access to (Amr Tolba, 2021).

iii. **Encryption**

Data encryption is a crucial technique used to protect sensitive information while it's being transmitted over networks or stored in databases. Encryption involves converting the plaintext to cipher text using encryption algorithms and encryption keys. Only authorized parties with the correct decryption keys can convert the cipher text back into readable plaintext. It's an essential component of ensuring the confidentiality and integrity of data both during transmission and while at rest (Yin et al., 2022).

iv. **Logging**

Application logs are records created by software programs to document different activities and events that take place while they are running. Logging gives useful information about how a program works, how users interact with it, and, in the event of a security breach, who may have gained unauthorized access or taken questionable actions. Logs provide vital information when security breaches occur. According to (Graham et al., 2016), logs aid in the following ways;

a. Forensic examination of logs can be used for forensic analysis to determine the chain of events leading up to a security breach when it happens. They help in determining the attack vector, the techniques employed, and the steps performed by the attacker.
b. Alerting and reviewing: Security teams can identify unusual patterns or anomalies that may point to an active breach by routinely reviewing application logs. Administrators can be alerted by automated alerts of potential security problems.
c. Logs can also assist in determining the root cause and the processes that lead to application failures or disruptions brought on by security breaches.

d. Application logs can help keep track of user activities, such as login attempts, data access, and other communications. This information is essential for spotting unauthorized or questionable activity.
e. Evidence for Investigations: In the wake of a security event, log data may be used as evidence in investigations or court cases. It helps create a timeline and provides a foundation for comprehending the breadth of the breach.

v. **Application security testing**

As defined by (Li, 2020), application Security Testing is a set of processes and techniques designed to identify vulnerabilities and weaknesses within software applications. It should be an ongoing process throughout the development lifecycle, including post-deployment maintenance. The goal of application security testing is to ensure that applications are resilient and secure against various cyber threats and attacks, preventing potential exploits and unauthorized access. It involves assessing the application's code, configurations, and overall architecture to identify potential security risks.

c) Information security

According to (Ogbanufe, 2021), Information security is the technique for preventing unauthorized access to, use of, disclosure of, interruption of, alteration of, or deletion of information. It involves protecting physical and digital data against misuse, unauthorized access and changes, and also deletion. It is used to safeguard the data, code, and other information that businesses collect from their customers and users. Confidentiality, Integrity, and Availability are the main requirements of information security.

d) **Operational security**

As defined by (Ogbanufe, 2021), operational security refers to a systematic approach used to identify, analyse, and protect sensitive information that could be used by attackers to compromise the confidentiality, integrity, and availability of the overall operation of an organization. It involves establishing and enforcing procedures and guidelines that dictate how data should be handled, accessed, stored, and shared. It ensures that all individuals within an organization are aware of their responsibilities and obligations regarding security.

It involves assessing the organization's activities, procedures, and information flows from the perspective of potential adversaries. This helps to identify vulnerabilities and potential attack vectors that could be exploited. The goal is to manage and control the release of information to ensure that sensitive data and critical operations are protected.

e) **Disaster Recovery Planning**

According to (Sicard, 2019), disaster recovery planning is the process that outlines how to continue working quickly and effectively following a calamity. It should start at the business level by identifying the apps and resources that are typically essential for carrying out the organization's operations.

f) **End User Security**

According to the global learnings system, “An end user is an employee who uses the software and hardware assets of an organization to perform their job duties”. It is therefore very important to understand what is happening in cyberspace. They should have the ability to recognize threats, and attacks and also report incidents. The IT Security of an organization relies heavily on the end user; therefore, security training should be a top priority for every organization. (Krishnasamy & Venkatachalam, 2023). According to Platview Technologies (2023), end-user best practices include;

i. Data classification and privacy: Workers and other computer users need to understand how data is categorized for usage and protection.
ii. Social engineering and anti-phishing: To understand what makes an email appear suspicious and what to do when they encounter one, users need phishing awareness training. They also need to be aware of typical social engineering techniques and tactics, as well as what they may do to safeguard their privacy and that of their data.
iii. Employees should be aware of the best practices for setting secure passwords and the password management guidelines (e.g., never share passwords, use passwords with at least eight characters, etc.).
iv. Antivirus Software: Using antivirus software is recommended for both people and businesses. Users need to understand the importance of never turning it off or running free antivirus software.
v. Use of VPNs: If an employee is permitted to access the networks and servers of their company from distant, off-site locations, they should be given a VPN and instructions on how to use it safely.

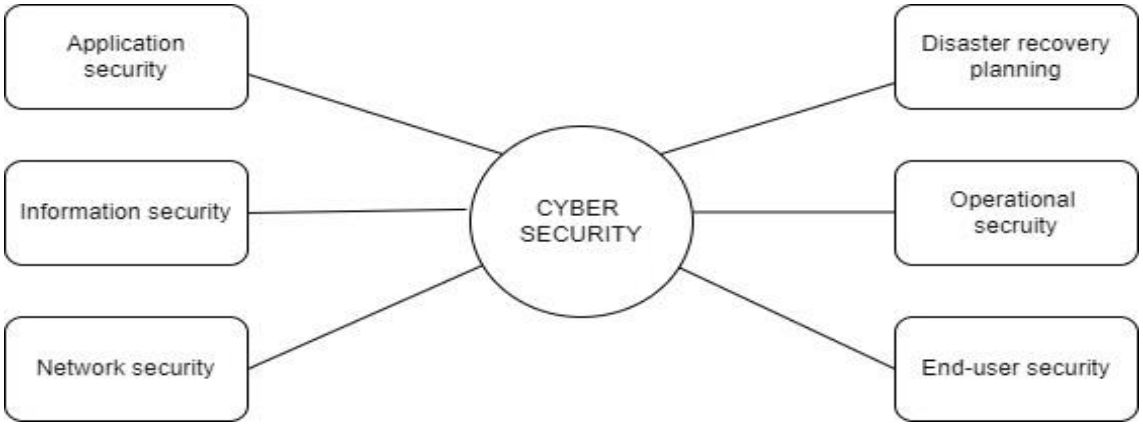


Figure 1. 2:**Elements of cybersecurity**

Source: cyber(swarnavo, 2022)

2.3.2 Cyber security Attack Surface

The attack surface represents the cumulative count of all potential points, known as attack vectors, through which an unauthorized user could potentially infiltrate a system and retrieve data. From an organization's perspective, an attack surface is the sum of vulnerabilities within the organization that hackers can use to gain unauthorized access to the information system environment or sensitive data to carry out a cyber-attack. According to Bobby (2022), the attack surface can be divided into three sub-surfaces namely; social engineering attack surface, digital attack surface, and physical attack surface.

a) Social Engineering Attack Surface

Uneducated People remain to be one of the greatest risks a business can have. Attackers only need to use social engineering and take advantage of human psychology to trick an employee. Social engineering tricks people into paying money to criminals, sending information they shouldn't transmit, installing software they shouldn't download, visiting websites they shouldn't visit, and other blunders that jeopardize their security or that of their organizations. Social engineering is frequently referred to as "human hacking" since it targets human weaknesses rather than flaws in technical or digital systems.(Plappert et al., 2021). Some ways an attacker uses to attack and access a company’s assets

a. An email phishing assault when a worker is duped into downloading malware by convincing them to open a malicious attachment or link
b. By pretending to be a service provider, such as a janitor or repairman, an attacker could physically access company assets

c. Media drops, which occur when an employee unintentionally plugs an infected USB stick into a computer at work.

b) Digital Attack Surface

The digital attack surface area encompasses all the hardware and software that connect to an organization's digital infrastructure. It exposes the organization's cloud and on-premises infrastructure to any hacker with an internet connection (Gordon et al., 2020).

According to (Das & Pathak, 2022), Some common digital attack surfaces include Weak passwords, Misconfiguration, Shared databases and directories, Outdated or obsolete devices, data, or applications, and Shadow IT.

i. **Weak passwords** entail the use of easily guessable, weak passwords. A significant finding from IBM's "Cost of a Data Breach Report 2021" was that compromised credentials became the most often used attack vector in 2021.

ii. **Misconfiguration** Hackers can enter networks using improperly configured network ports, channels, wireless access points, firewalls, or protocols. Man-in-the-middle attacks, for instance, use lax encryption algorithms on message-passing channels to eavesdrop on system conversations

iii. **Shared databases and Directories**- To access critical resources without authorization, hackers use databases and directories that are shared between systems and devices.

iv. Another digital attack surface that is vulnerable because updates and patches are not consistently applied is **outdated hardware or software.**

v. **Shadow IT**: Employees who use software, hardware, or gadgets without the IT department's knowledge or consent. Because security professionals aren't monitoring it, it could present significant flaws that hackers could exploit.

c) Physical attack surface

The physical attack surface encompasses all endpoint devices that an attacker can gain physical access to, including but not limited to Universal Serial Bus drives, desktop computers, laptops, mobile phones, IoT devices, and hard drives. According to (Plappert et al., 2021), the physical attack threat surface includes Malicious insiders, Device theft and Baiting,

i. **Malicious insiders**: bribed workers or other users may abuse their access rights to steal important information, disable devices, plant malware, or worse.

ii. **Device theft:** By breaking into a company's offices, criminals may take endpoint devices or obtain access to them. Hackers can access data and processes stored on these devices once they have the hardware. They could even access additional network resources by using the identity and authorization of the device. The typical targets of theft are endpoints utilized by remote workers, employees' devices, and improperly dumped equipment.

iii. **Baiting:** In this type of attack, hackers leave malicious USB drives in public locations to lure people into inserting the drives into their computers and unintentionally installing the virus.

2.4 Cybersecurity Risk

As defined by (Gordon et al., 2020), Cybersecurity risk encompasses the potential for financial losses, disruptions, or harm to a firm's reputation arising from the breakdown of its information technology systems due to external attacks. According to (Kure et al., 2022), risk is the potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability. A threat is anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset (i.e. A threat is what we're trying to protect against). Vulnerability is a weakness or gap in a security system that can be exploited by threats to gain unauthorized access to an asset.

An asset encompasses People, property, and information belonging to an institution or an individual. People include and not limited to employees and customers along with other invited persons such as contractors or guests. Property assets consist of both tangible and intangible items that can be assigned a value. While intangible assets include reputation and proprietary information such as databases, software code, critical company records, and many other intangible items. Based on Kure and Islam's (2019) definition of cyber security "risk is the potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability". Then this can be reduced to the following formula

$R = (T + V + A)/ C$

Where:

R is Risk (*Risk is the intersection of assets, threats, and vulnerabilities*), ***T*** is Threat

(*threat is what we're trying to protect against*), ***V*** is vulnerability (*vulnerability is a weakness or gap in our protection efforts*), ***A*** is Asset (*An asset is what we're trying to protect*) while ***C*** is a countermeasure (*which represents the protection efforts put in place to ensure that assets are safe from cybersecurity incidences*).

2.4.1 Elements of risks

Threat, vulnerability, consequence, and asset value are the four elements that commonly make up the definition of cybersecurity risk. (Kure et al., 2022)

i. **Threats**

As stated in the research by Victoire et al. (2023), a cyber-security threat is defined as any potential malicious attack to acquire unauthorized access to data, disrupt digital operations, or compromise information integrity. These cyber-threats can originate from various sources, including corporate espionage, hacktivists, terrorist groups, hostile nation-states, criminal syndicates, individual hackers, and dissatisfied employees.

Several threat examples encompass advanced persistent threats, distributed denial of service (DDoS) attacks, and social engineering attacks. Threat actors are often motivated by financial profit or political aspirations, and they can be linked to nation-states, insiders, or criminal groups. Recognizing these threats is crucial in the realm of risk management to effectively combat cyberattacks within organizations. However, due to the unpredictability of cyberattacks, accurate risk perception is essential. According to a research survey conducted by Kure et al. (2022), having a precise understanding of risks such as denial of service, cyber espionage, and crimeware from the threat perspective can assist organizations in identifying the most effective controls to manage these risks.

Threats come in two primary categories: outsider threats and insider threats. Both of these categories carry significant risks for a company and have the potential to lead to serious system attacks. External attackers typically face more challenges when attempting to compromise the security system. On the other hand, insiders are individuals with authorized access to the company's system, which grants them easy access to data that they could potentially steal or share. Examples of insider threats encompass employees, staff, workforce members, and business associates, while outsider threats consist of hackers, unidentified external individuals, and ransomware attackers (Lee, 2022; Sav & Magar, 2021).

a. Insider threat

The insider threat is often described as the adversary within the fortress. Underestimating the consequences of insider threats is no longer acceptable. Organizations, institutions, and government entities must adopt a robust security culture. According to Kaspersky (2023), even

well-established businesses like Tesla, which suffered from acts of sabotage and intellectual property theft, and Capital One, which fell victim to fraud, have had to confront the reality of insider threats. Furthermore, the data breach at the US Department of Defense, orchestrated by notorious individuals like Chelsea Manning and Edward Snowden, who are renowned for their espionage and hacktivist activities, had far-reaching social implications (Mazzarolo & Jurcut, 2019).

According to a recent analysis published in early 2020 by the Ponemon Institute, there has been a 47% increase in the frequency of insider threat incidents since 2018. Moreover, the average global cost associated with these incidents has risen by 31%, reaching $11.45 million. The research underscores that insider threats persist as a recurring, often underestimated, and frequently unaddressed cybersecurity concern within organizations across North America (including the United States and Canada), Europe, the Middle East & Africa, and the AsiaPacific region. This conclusion is drawn from interviews conducted with IT security practitioners in 204 organizations, as reported by Georgiadou et al. (2022).

A study conducted by the cybersecurity company Tessian during the COVID-19 pandemic revealed that 78% of IT leaders hold the belief that their organization becomes more susceptible to insider attacks when employees work remotely. The COVID-19 crisis and ongoing shifts in business practices have given rise to a "remote" or "hybrid" work environment, exposing individuals to a greater degree of both internal and external pressures. As noted by Maghlaperidze et al. (2021), such situations not only provide opportunities but often exacerbate incidents related to insider threats, as they create the necessary technical, social, economic, and psychological conditions for these threats to flourish.

As stated by Georgiadou et al. (2022), various technical papers have identified, analyzed, and presented the primary insider threat types and their subcategories. It's worth noting that these attack techniques can vary depending on the specific industry or sector in question.

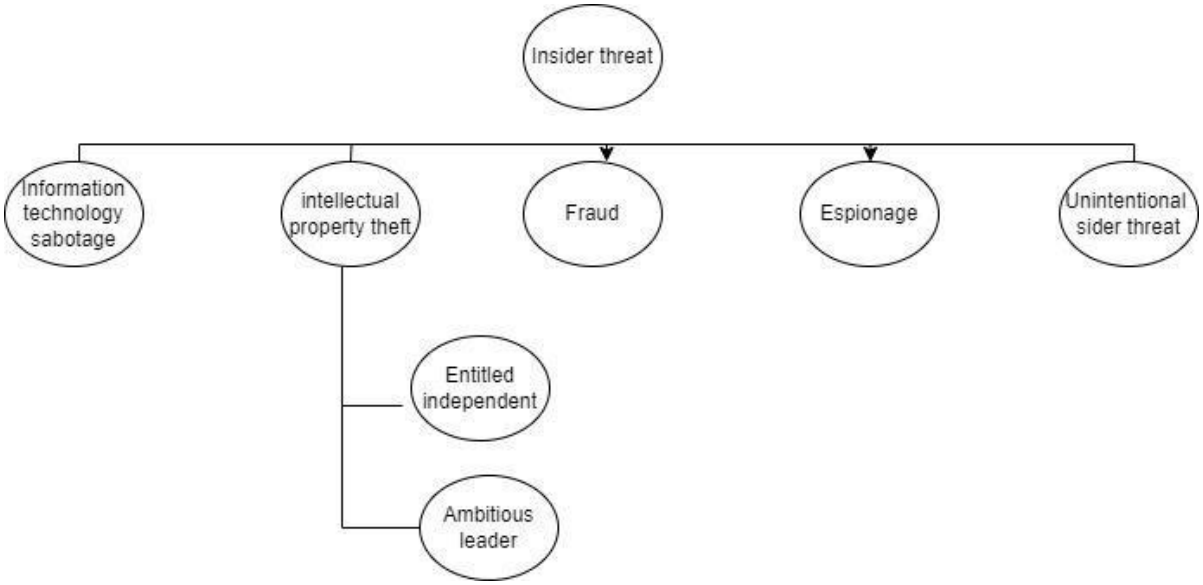


Figure 2. 1: **Types of insider threats**

Source:(Mazzarolo & Jurcut, 2019)

i. Information technology (IT) sabotage is the use of IT to specifically harm a person or an organization.(Greitzer et al., 2019)

ii. Intellectual Property (IP) Theft: Using one's credentials improperly to steal proprietary or private information from the company (Georgiadou et al., 2022).

- Entitled Independent: An insider functioning solely on his or her own to steal information to use in a new position or for a side enterprise.
- Ambitious leader Recruits insiders to steal information for a greater purpose iii. Fraud is the unauthorized alteration, addition, or deletion of data held e.g. identity theft and credit card fraud(Greitzer, 2019)

iv. Espionage is the act of obtaining, providing, sending, receiving, or sharing information concerning the nation's defense with the intent or reasonable suspicion that the knowledge may be used against one's own country or in favor of any other country.(Georgiadou et al., 2022)

v. Unintentional insider threat: Using action or inaction without malicious intent, negatively impacting the confidentiality, availability, or integrity of an organization's information or information systems.(Georgiadou et al., 2022)

b. Outsider Threats

As indicated by Lee (2022), outsiders, including hackers, unidentified external individuals, and ransomware attackers, exemplify the category of outsider threats. These external threats occur regularly and possess the potential to inflict significant damage on various entities such as

businesses, governments, and hospitals. The extent of the harm incurred depends on factors such as the nature of the attack, the tactics employed, and the motivations driving the attackers. For instance, in the case of a financially motivated assault targeting a company, the primary objective of the hackers is to secure the funds and make a swift exit.

In the realm of hacktivism, hackers may follow a different approach by initially attempting to acquire confidential information before deliberately causing harm to a company's operations or reputation. As a result, some outsider threats can pose more significant dangers than others, depending on the specific organization, its industry, and the robustness of its current cybersecurity infrastructure. To mitigate the risks associated with outsider threats, Sangfor Technologies (2023) recommends several key measures. These include regular updates of security systems, providing staff training to enhance their ability to detect and respond to these attacks, and the adoption of cybersecurity solutions from reputable vendors like Sangfor. Furthermore, they emphasize the importance of securing data, applications, and servers through the implementation of tools such as network detection and response, web gateways, filtering solutions, and firewalls. These steps collectively contribute to a more resilient defense against outsider threats.

Threats can also be categorized as either direct or indirect threats. The words "direct threats" and "indirect threats" are frequently used in the context of cybersecurity to define various hazards and assaults that target computer systems, networks, and data. These words aid in distinguishing between threats that directly take advantage of weaknesses and those that may indirectly result in security breaches(Alghamdi, 2021).

According to (Joachim Bjørge Ulven, 2021), a thorough hybrid model for threat classification is dubbed the "multi-dimensions' model for threat classification." The basic goal behind their approach, they claim, is to incorporate several classification criteria put out by others and illustrate their potential impact because other researchers have not been able to provide an entire list and categorization of risks. As shown in Figure 3 below, a multi-dimension model of categorization classifies threats based on their source, threat agents, motivation, aim, and impact.

Threats in the realm of cybersecurity are often categorized as either direct or indirect threats. These terms are frequently employed to describe various hazards and attacks targeting computer systems, networks, and data. They serve the purpose of distinguishing between threats that directly exploit vulnerabilities and those that may indirectly lead to security breaches, as highlighted by Alghamdi (2021).

Additionally, in the work of Joachim Bjørge Ulven (2021), a comprehensive hybrid model for threat classification is introduced, referred to as the "multi-dimensions' model for threat classification." The primary objective of this approach is to integrate various classification criteria proposed by others and elucidate their potential impact. This model, as depicted in Figure 4, categorizes threats based on multiple dimensions, including their source, threat agents, motivation, objectives, and impact. This comprehensive approach aims to provide a more thorough and holistic understanding of the diverse nature of threats in cybersecurity.

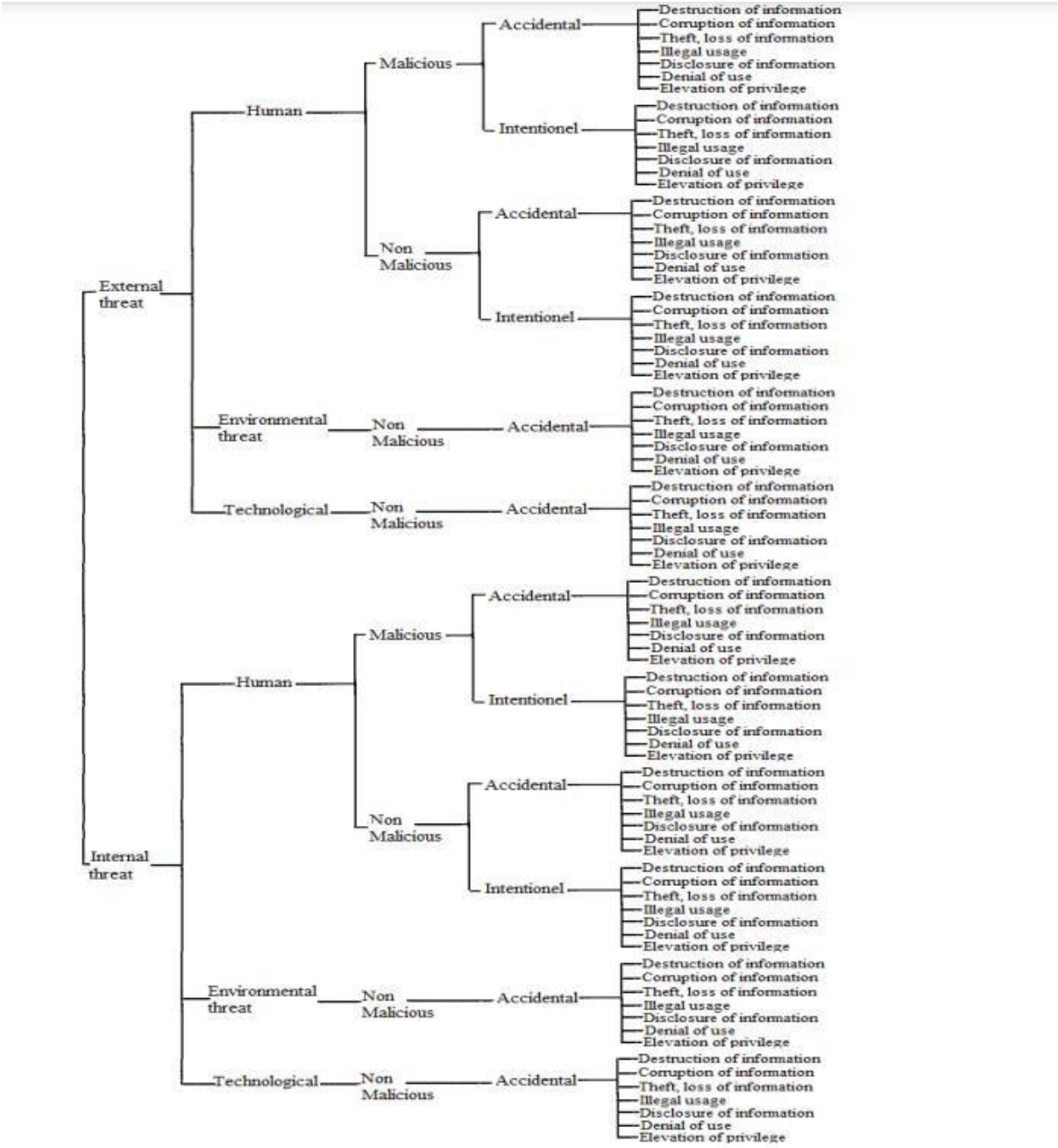


Figure 2. 2: **multi-dimensions threat classification model**

Source: **(Sav & Magar, 2021)**

a. Direct Threats

Direct threats are active and purposeful, and directly aimed at exploiting system or network vulnerabilities with the direct goal of compromising, tampering with, disrupting, stealing or manipulating data, services, or resources. These attacks opportunely exploit vulnerabilities of security so as to attain malicious motives. X. Liu et al. (2022) refer to direct threats represented by malware (including viruses, worms, Trojans, ransomware, and spyware) as the most frequent manifestations of direct threats that infect and damage the computer

systems directly. Phishing is also similar: any type of fraud which is aimed to make a user share some confidential information with a third party, such as a password, financial data, and others, and accessing them without authorization. Denial of Service (DoS) attacks also fits in this group because they overwhelm system, net or a particular service with too many requests making them unavailable to lawful users.

In addition to bloodthirsty attacks against specific users, other manifestations of direct threats may be the leakage of data, the hacking of which does not violate the confidentiality and privacy of information, but often has a harsh legal and financial outcome (X. Liu et al., 2022). Another risk category is exploits, which are used in order to achieve unauthorized task control of systems by discovering software vulnerabilities. Insider threats are especially dangerous, since they occur at a low level, through the machinations of the trusted members of the organization who are able to engineer a breach of security internally. These direct threats alone represent a considerable challenge to cybersecurity and it is therefore vital to have adequate preventive measures, constant monitoring and a rapid response to the occurrence of cyber incidents to curb the effects of the threats to organizations and individuals.

b. Indirect Threats

Indirect threats, referred to as contributing factors or secondary threats, do not directly exploit vulnerabilities but can elevate the likelihood or consequences of direct threats. These threats can create an environment that fosters cyberattacks. As noted by Sav & Magar (2021), examples of indirect threats include:

a. Weak Password Policies: Inadequate password policies indirectly increase the risk of unauthorized access by making it easier for attackers to guess or crack passwords.
b. Lack of Security Awareness: Users who are not aware of security best practices are more likely to fall for social engineering attacks, indirectly increasing the risk of breaches.
c. Outdated Software: Using outdated software indirectly exposes systems to known vulnerabilities that have not been patched.
d. Poor Network Segmentation: Inadequate network segmentation can indirectly enable lateral movement for attackers within a network.
e. Lack of Regular Backups: Failing to regularly backup data indirectly increases the risk of data loss in case of a ransomware attack.

Both direct and indirect threats contribute to the overall cybersecurity landscape and the potential for breaches. Addressing both types of threats is important for maintaining a strong security posture and effectively safeguarding digital assets and information.

ii.**Vulnerabilities**

A vulnerability is essentially a weakness within an information system, system security processes, internal controls, or implementation that has the potential to be exploited or triggered by a threat source, as explained by Lee (2022). These vulnerabilities can be exploited in various ways, making vulnerability management a critical practice for staying ahead of potential attackers. An analysis of Human Factors in Electronic Health Records Cybersecurity Breaches, conducted by Nifakos et al. (2021), revealed that data breaches in the healthcare industry were primarily attributed to unintentional human factors. These factors include carelessness, negligence, and falling victim to phishing and ransomware attacks, and they outnumber breaches caused by malicious intent. This underscores the importance of addressing human vulnerabilities in the context of cybersecurity.

The study conducted by Yeo and Banfield (2022) provides valuable insights into the prevalence and causes of cybersecurity breaches in the healthcare sector. Between January 2015 and December 2020, a total of 1,485 breaches affected a staggering 141,252,797 medical records. Notably, malevolent actors were responsible for 26.7% of these breaches, which had a significant impact on 73.1% of all the affected records. The research findings also highlight the primary reasons behind cyber-breach occurrences in organizations. Carelessness and negligence accounted for the highest number of incidents, totalling 382 instances. Theft followed as the second most frequent cause, with 222 incidents, and falling victim to phishing scams was the third most common cause, with 221 incidents. These findings underscore the critical role that human factors, such as carelessness and susceptibility to social engineering attacks, play in cybersecurity breaches. The four main types of security vulnerabilities are; Network vulnerabilities, System vulnerabilities, Human vulnerabilities, and Process vulnerabilities.

a. Network vulnerabilities

Network vulnerabilities are essentially gaps in an organization's hardware, software, or overall infrastructure that can be exploited by cyber attackers. These vulnerabilities create opportunities for unauthorized access, data breaches, service disruptions, or other harmful activities. The range of vulnerabilities can span from relatively simple issues like weak passwords to more complex ones involving misconfigured or poorly secured network components. Network vulnerabilities entail the following;(Tufail et al., 2021).

i. Range of Exposure: Network vulnerabilities cover a broad range of potential flaws that attackers may exploit. This can include unpatched software, routers that are not properly configured, insecure wireless access points, and more.

ii. Unauthorized Access: Attackers use these flaws to access systems, applications, or data that they are not authorized to access. Data theft, data modification, or even total control over hacked systems are possible as a result.

iii. Harmful Consequences: Attackers can seriously harm an organization if they have taken advantage of these weaknesses. Financial losses, reputational impact, legal repercussions, and business interruption are just a few examples of how this harm can appear.

iv. Strategies for Mitigation: To reduce the risk of exploitation, organizations need to aggressively identify and remedy vulnerabilities. This entails doing security audits, patch management, and vulnerability assessments regularly.

v. Defense Mechanisms: Employing a variety of security measures, including as tight access restrictions, firewalls, intrusion detection and prevention systems, and employee security awareness training, is necessary for an effective defense against network vulnerabilities.

vi. Continuous Monitoring: Because the cybersecurity landscape is continually changing, businesses must regularly check their networks for attacks and new vulnerabilities. To lessen the potential impact of assaults, prompt notice and action are essential.

vii. Collaboration: When addressing network vulnerabilities, an organization's management, security, and IT teams must frequently work together. To achieve an allencompassing and well-coordinated security policy, everyone must cooperate.

viii. Third-Party Risks: Organizations also need to consider vulnerabilities that might exist in their third-party vendors or partners' systems. An organization's security is only as strong as the weakest link in the supply chain.

b. System vulnerabilities

Operating-system (OS) vulnerabilities are a form of security gap that an adversary can use to circumvent system integrity, confidentiality or availability. The types of attack include Denial of Service (DoS), Distributed Denial of Service (DDoS), Remote Code Execution (RCE), and privilege escalation which allow the attackers access to disrupt services to the users, gain access, or take control of full of all the system. The hazards increase when the systems parametrization adopted by organizations is obsolete or unpatched, since such

configurations are often well known to be vulnerable and easily exploitable. To remain resilient and reduce exposure to a security threat, mitigation requires periodic patching, powerful intrusion-detection systems, and multilayered defense to achieve security controls (Ansari et al., 2022; Sharma and Saini, 2021).

c. Human vulnerabilities

Human susceptibilities are a major security risk to cybersecurity as the human element has the power to interfere with the networks, hardware, and other sensitive data due to mistakes or carelessness. The increasing risk of off-site and mobile employment has only added to this exposure typically in the form of opening suspicious email and although it might initially seem like it the failure to update necessary software. The studies have shown that more than 39% of all security risks arise directly, in relation to human conducts, meanwhile 95 percent of all successful cyberattacks are all orchestrated by human beings, and the major owners of such attacks are humankind, mainly, through insider threats (Nifakos et al., 2021). The main factor that leads to such vulnerability is the user awareness on cyber risks that even with several security measures and user training programs, the attacker can take advantage to exploit their cognitive biases and trust tendencies (Alsharif et al., 2021; Abebe, 2020).

There are multiple tactics to exploit human weaknesses used by cybercriminals, but among them, social engineering is the most powerful tactic; it is the one that is used to achieve about 95 percent of web attacks (Alsharif et al., 2021). This practice tricks people into sharing secretive data assuming they are trusted parties over the phone, by email or even during a face-to-face meeting. Its major variants involve phishing, i.e., attackers sending someone deceiving mail with malicious links or attachments, spear phishing, which is aimed at particular individuals or organizations with the help of personalized information, baiting, i.e., seemingly valuable objects that have a malicious code on a USB disk or a software that can be acquired as a result of pretexting, i.e., hackers creating a pretense to obtain reserved data in bad faith. All these strategies coupled with the calculated dynamic nature of human related cyber threats emphasize the need to keep educating users, awareness programs, and behavioral risk reduction systems in place.

d. Process vulnerabilities.

Refer to gaps in the operational procedures that an organization uses to secure its systems, data, and networks. An authentication flaw when users and even IT managers utilize weak passwords is among the most prevalent process weaknesses. These vulnerabilities can result from poor design, inadequate implementation, lack of updates, or improper execution of security processes.(Tufail et al., 2021)

iii. **Countermeasures**

Security countermeasures encompass a set of measures and controls used to ensure the confidentiality, integrity, and availability of data and information systems. These measures include technological safeguards, policies and procedures, adherence to standards, compliance with regulations and legislation, and the adoption of advanced security protocols. For example, multi-factor authentication and specialized software tools are employed to enhance security, while clear and comprehensive security policies guide users on safe data handling. Additionally, compliance with industry-specific standards and government regulations is vital, and in emerging technologies like the Internet of Things (IoT), cryptographic security protocols are used to safeguard devices and data. In complex environments like smart cities, a smart governance architecture, along with multi-level security controls, is imperative to address diverse security challenges effectively (ITU Telecom World, 2021).

a. Technological countermeasures

Countermeasures that involve the use of technology form an essential part of a comprehensive cybersecurity infrastructure and provide both preemptive and retrospective systems to protect information programs against a broad attack range of cyber threats (Salami Pargoo and Ilbeigi, 2023). Based on more sophisticated tools and techniques, they protect networks, systems, data and endpoints, limiting the likelihood of any attacks. Some of the most commonly used measures include firewalls that filter unauthorized traffic, intrusion detection and prevention systems (IDPS) which alert and block the malicious operations in real-time, and anti-virus or antimalware programs that are used to locate and eliminate harmful code (Boeding et al., 2022). Data protection is enhanced by encryption that makes data unusable without decrypting tools and endpoint protection that keeps any user devices out of reach of users.

Advanced protection mechanisms have been developed in the modern day cybersecurity with the intention to reinforce defense. Behavioral analytics allows detecting unusual behavior that indicates an impending breach, and mobile device management (MDM) systems impose a rule onto portable devices and remotely rectify the threats. WAFs block specific exploits directly targeting online platforms and backup and disaster recovery solutions can be used to maintain the ability to work under conditions of disaster. Facial recognition and fingerprint scan methods of authentication enhance identity checking, the access control is much enhanced, as compared to common password. Taken together, these

countermeasures form a tiered defense approach that is a necessary part of a modern cybersecurity resilience (Salami Pargoo & Ilbeigi, 2023; Boeding et al., 2022).

b. Policies and procedures

Policies and procedures constitute a crucial component of a robust cybersecurity model. They serve as guidelines for employees, consultants, partners, board members, and other end users, outlining specific cybersecurity protocols to be followed when communicating data over networks, accessing online resources, and engaging in other security-related activities. The SANS templates provide various policy examples, including remote access, wireless communication, password protection, email, and digital signature policies. Cybersecurity policies, especially for large firms or those operating in regulated industries, can be extensive, spanning multiple pages to comprehensively address security concerns. In contrast, small businesses may have shorter policies covering fundamental safety measures, as described by Trellix (2023). These techniques and policies could encompass guidelines for email encryption, how to access work applications from a distance, instructions for creating and protecting passwords, and guidelines for using social media.

c. Standards

Cybersecurity standards serve as a valuable resource for organizations aiming to bolster their cybersecurity posture. These standards encompass a set of rules or best practices designed to guide establishing effective defenses against online threats, safeguarding systems and data, and managing cybersecurity incidents. By adhering to cybersecurity standards, businesses can identify and implement the appropriate security measures tailored to their specific needs, as well as gain insights into how to effectively handle and recover from cybersecurity events. The ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, ISO/IEC 27006, and ISO/IEC 27007 standards make up this collection.(Tissir et al., 2021)

i. Common Criteria (ISO/IEC 15408): This standard primarily addresses IT product certification. It guarantees that IT products will be judged by a set of criteria that are strictly adhered to by business and government. The three sections that makeup ISO/IEC 15408 are Part 1 (Introduction and general model), Part 2 (Security functional requirements), and Part 3 (Security assurance requirements). Another document used by security auditors to assess IT products is the Common Evaluation Methodology (CEM).

ii. This standard, SO/IEC 18043, supports an organization's IT infrastructure in the selection, deployment, and management of intrusion detection systems.

iii. Based on ISO/IEC 27001 and ISO/IEC 27002, ISO/IEC 27017 addresses the cloud controls that apply to cloud service providers.

iv. Concerning the disclosure of vulnerabilities in IT goods and services, there is ISO/IEC 29147. It offers providers advice and suggestions for managing technical vulnerabilities.

v. Concerning procedures for handling vulnerabilities, ISO/IEC 30111. It offers specifications and suggestions for handling and fixing vulnerabilities in IT products.

vi. The ISO/IEC 27037 standard outlines procedures for identifying, gathering, acquiring, and preserving digital evidence.

vii. PCI DSS: Payment Card Industry Data Security Standard The standards for vendors and financial institutions to process credit card payments securely are outlined in this document.

viii. The non-profit group Cloud Security Alliance (CSA) routinely releases the best security procedures for cloud security.

d. Regulations

Cybersecurity regulations encompass directives aimed at safeguarding computer systems and information services against a range of threats, including denial-of-service (DOS) attacks, unauthorized access (such as theft of confidential or intellectual property), and control system attacks, as described by Wikipedia (2023). To prevent cyberattacks, various cybersecurity measures can be implemented. These include the use of firewalls, antivirus software, intrusion detection and prevention systems, encryption techniques, and strong login passwords. Additionally, collaborative efforts between the public and private sectors have been initiated to promote voluntary cybersecurity enhancements and address the evolving threat landscape. Notably, industry authorities, particularly banking regulators, have recognized the significance of cybersecurity threats and have either incorporated cybersecurity considerations into their regulations or have plans to do so in the future. This reflects the growing importance of cybersecurity in today's digital age.

e. Legislation

Also known as internet laws, cyber laws are a body of law allotting to legal law of informatics that regulates the use of software, e-commerce, information security, and the digital transmission of information in aspects like internet access, freedom of speech and privacy (Narasimman, 2023). Their major goal is to prevent cyber crimes and making sure that computer systems and the use of online platforms are legal and ethical. Key areas are fraud prevention, ensuring that people are not subjected to identity thefts, credit-card fraud,

among other crimes that are subject to federal and state prosecution; copyright protection, where the abuse of copyrights is prevented and copyright holders and associated entities can protect and make money of their intellectual property; and defamation check, whereby online slander is addressed and a platform against defamation online.

iv. Asset Value

Asset valuation is a method used to determine the value of an organization's information system assets, and it is typically based on the principles of confidentiality, integrity, and availability (CIA), as outlined by Yang et al. (2022). The calculation for total asset value involves multiplying the asset value by its assigned weight:

Asset Value * Asset Weight = Total Asset Value.

According to (Septiani et al., 2022), Several assumptions and considerations are made in the process of asset valuation:

- The value of an asset is influenced by the sensitivity of the data it holds and the potential impact on the CIA triad (confidentiality, integrity, and availability).
- Each piece of information is assigned a minimum value of 1.
- The CIA triad is assessed using a rating system where a value of 1 represents low, 2 is medium, and 3 indicates high.
- The total value of the asset is determined by the sum of the three qualities (C + I + A) based on the CIA rating.

In the context of ISO/IEC 27001:2005 standards, assets are defined as "anything that has value to the organization." This definition encompasses a broad range of elements that contribute value to the organization, including personnel, infrastructure, outsourced services, hardware, software, and electronic information, as highlighted by Kure & Islam (2019).

2.4.2 Building Blocks of secure cyber space

According to (Alejandro, 2022), The foundation of a secure cyberspace is built upon three key building blocks: people, processes, and technology. In recent years, the frequency of security breaches involving sensitive data, such as personal information, has become a recurring phenomenon. These building blocks work together to establish a robust cybersecurity model and protect against these breaches.

2.4.2.1 people

In addition to any technological measures introduced to mitigate security breaches, human factors remain an often-neglected aspect. The assumption that individuals will consistently adhere to established security procedures and rules is frequently unfounded. Human factors

undoubtedly remain a critical element in information security. It is essential to assess whether there exists a cybersecurity-aware culture among individuals if roles and responsibilities are well-defined, and if the organization's hierarchy reflects the significance of cybersecurity. (Lartey, 2021).

Perpetrators of data breaches are increasingly recognizing human factors as a vulnerability in information security for their successful operations (Gonzalez & Sawicka, 2023). Research indicates that organizations often underestimate the role of human factors as a primary contributor to security breaches. The organization's staff members also play a significant role in contributing to security breaches (Lartey, 2021).

Regardless of the scope, design, and implementation of any security system, it ultimately relies on individuals. The safeguarding of personal data hinges on a robust information security plan that unequivocally addresses human factors. (Gonzalez & Sawicka, 2023).

2.4.2.2 Processes

Government policies and also legislation are key building blocks in ensuring a secure cyberspace, but this must be accompanied by defining obligations and liabilities to increase implementation and enforcement. (ITU Telecom World, 2021)

The establishment of a robust cybersecurity model necessitates the implementation of secure cybersecurity regulations. These regulations are essential to safeguard information technology and computer systems, compelling organizations to fortify their defenses against a myriad of cyber threats, including viruses, Trojan horses, denial of service attacks, illegal access, and more (Srinivas et al., 2019).

In addition to government policies and legislation, processes are fundamental building blocks in ensuring a secure cyberspace. However, it's imperative to complement these regulations with well-defined obligations and liabilities to enhance the implementation and enforcement of cybersecurity measures (ITU Telecom World, 2021).

Effective processes encompass not only legal models but also comprehensive procedures and protocols within organizations. These internal processes guide how security measures are applied, monitored, and enforced, covering aspects like access control, incident response, risk management, and compliance. Furthermore, processes ensure that cybersecurity is not merely a regulatory requirement but a systematic and ingrained practice, fostering a proactive approach to security.

2.4.2.3 Technology

Technology is a foundational building block in the realm of cybersecurity. It serves as a fundamental pillar for safeguarding systems, networks, and data in the digital age. The

selection and deployment of cybersecurity technologies are paramount. Several key considerations should be taken into account in this regard. These include delving into cryptographic and cryptanalysis research, and associated aspects. It's essential to focus on effective network security, encompassing both wired and wireless networks, as well as radiobased communication security. System security, incorporating cutting-edge biometrics, plays a pivotal role in bolstering defenses. Additionally, attention should be given to the development of enhanced security architectures (Samtani et al., 2020).

Monitoring and surveillance tools are indispensable for continuous vigilance, and cyber forensics capabilities are vital for investigating and understanding security incidents. Malware analysis tools aid in identifying and combating malicious software. Identity management systems are crucial for authenticating and authorizing users. Situational awareness and attack attribution technologies provide insights into ongoing threats. The survivability of critical systems and networks is of paramount importance, along with the development of scalable and trustworthy systems and networks (Qin et al., 2021).

Furthermore, these technologies should not exist in isolation but should be integrated into a cohesive cybersecurity strategy. They serve as the technical underpinning of cybersecurity efforts, working in synergy with people and processes to fortify an organization's defenses against an ever-evolving cyber threat landscape.

2.5 Human factors in cybersecurity

Cybersecurity is a combination of the vulnerabilities that exist in the cyberspace and the attempts to protect it. The cyber-attack theory states that the effectiveness of this undertaking largely depends on the information that attackers have before the operation and any information they obtain or tamper with in the process (Liu et al., 2022). The field is essentially involved in the maintenance of the confidentiality, integrity and availability of computing resources both internally and externally in the organization networks. Although cybersecurity has generally focused on technical features, including encryption, network defense, or algorithmic security, academics portray cybersecurity as going beyond technical solutions to have a combination of data, systems and actors (Suryatrisongko & Musashi, 2019). In the absence of multidisciplinary views, even the strongest technical safeguards cannot be considered adequate, as it is clear by the persistent increase in cyber-attacks (S vabensk y, 2020).

Human factor is a decisive element in the field of cybersecurity as it influences the number of vulnerabilities, and the choice of proper defense mechanism. User awareness, user

behavior patterns, password implementation related practices, susceptibility to social engineering attacks, insider threats, user ignorance, mobile devices, user mobility, and organizational culture are some of the variables that combinedly condition the security stance of an organization. An intensive approach encompassing integration of both technological solutions and teaching activities, implementation of policies, and changes in culture is essential in proper remediation. Through integration of aspects of human factors into the overall cybersecurity strategy, companies will become more resilient, reduce risks and improve their capacity to respond to the changing threat field in the ever-changing cyber realm.

2.5.1 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 (Dash & Ansari, 2022).

2.5.2 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 (Zimmermann & Renaud, 2019).

2.5.3 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 (S. Shyam Sundar, 2019).

2.5.4 Social Engineering

Social engineering continues to be one of the biggest human-factor flaws in cybersecurity as it entirely depends on psychological manipulation of the target to make them give out confidential information, perform actions that compromise their security. Human weaknesses, which include trust, curiosity, and willingness to help, are the paths cybercriminals follow by using such methods as phishing, where lies hidden under the guise of trusted sources persuade users to betray confidential information; pretexting, which hinges on made-up pretences; baiting, in which tempting but malicious files are used to trick users to download malware; and tailgating, when criminals get physical access to

secure facilities through adhering to social habits of courtesy and trust. All these tactics help to bypass the protection of the technology by utilizing the human factor, which makes them hard to detect and prevent in particular.

The possibility of counteracting the social engineering threats requires a comprehensive approach combining human education, technology, and policy implementations in organizations. Awareness programs among the staff members will be crucial in training the employees to detect suspicious contacts, checking information requests and acting accordingly to appropriately deal with a possible attack. More sophisticated email filtering and Multi-Factor Authentication (MFA) would be able to detect any phishing attempts; and generate additional verification levels to deny the unauthorized access to the system. Besides, contained security policies that are clear and enforceable and an effective incident response plan will ensure that threats are dealt with promptly first to reduce the level of damage. All these together help an organization become resilient to these manipulative cyberattacks that target human behavior, which makes continuing vigilance and dynamic cyberdefense keys to contemporary cybersecurity practice effective (Grassegger & Nedbal, 2021).

2.5.5 Insider Threats

One of the inherent human aspects concerning cybersecurity is insider threat, as this type of threat is generated inside an organisation, where the culprits have privileged access to its systems, networks, and data (Mazzarolo & Jurcut, 2019). These threats can be broadly characterised into two groups: malicious insiders- the ones who knowingly act with the aim of compromising by stealing data or sabotaging the system or admitting to espionage and unintentional insiders- these people unknowingly trigger security breaches in their actions that can range as low as falling the prey to phishing attacks to negligence involving compromised data or creation of errors exposing their systems vulnerabilities. Due to the level of knowledge internal to their company that malicious insiders have, they are extremely tough to find and even after being found, they are a problem that cannot be prevented easily because of the unanticipated security lapses that they might commit due to shock. Unintentional insiders however, are a problem that cannot be solved quickly as they still create a consistent threat.

Organizations should be able to mitigate the existing insider threats with a multi-level architecture that includes technical protection, procedures mechanisms, and human-oriented interventions (Greitzer, 2019). The main interventions would be the implementation of role-based access control (RBAC) designed to limit privilege to the

minimum level required to perform the assigned tasks as well as the implementation of continuous monitoring and auditing via Security Information and Event Management (SIEM) systems and user behavior analytics that would help detect variation in expected activity patterns. The complementary activities include thorough training and awareness of employees on how to avoid inadvertent novelties and properly developed incident response strategies that would allow immediate containment and remediation of incidents involving rogue insiders. All these help reinforces organizational resilience and reduce the probability and consequences of the insider threats.

2.5.6 Human Error

Human errors represent a significant human factor in cybersecurity. These errors encompass a range of actions or oversights by employees that can inadvertently lead to security incidents. Some common examples include misconfigurations of systems or applications, accidental data leaks, and neglecting to apply essential security updates and patches. They are particularly concerning because they can result from oversight, carelessness, or a lack of awareness rather than malicious intent. However, their consequences can be severe, potentially leading to data breaches, system vulnerabilities, or unauthorized access to sensitive information.

To mitigate the impact of human errors, organizations should implement proactive measures. Regular training and education programs can raise employees' awareness of common pitfalls and best practices to avoid errors. Automated security checks and validation processes can help identify and rectify misconfigurations or vulnerabilities before they are exploited. Streamlined and well-documented processes for implementing security updates and patches can also reduce the likelihood of errors. Moreover, fostering a culture of accountability and reporting within the organization encourages employees to promptly address and report any mistakes, allowing for timely corrective actions. Human errors are a prevalent human factor in cybersecurity, but organizations can minimize their impact through training, automated checks, and improved processes. These efforts contribute to a more resilient cybersecurity posture and reduce vulnerabilities stemming from human-related errors (Hadlington, 2021).

2.5.7 BYOD (Bring Your Own Device) and Workforce Mobility

According to (Wani et al., 2022), in the era of remote work and the widespread adoption of BYOD (Bring Your Device) policies, securing remote access and ensuring that employees follow secure practices outside the office have become paramount. These human factors significantly impact an organization's cybersecurity posture. As employees increasingly

use their devices for work-related tasks, such as accessing corporate networks and sensitive data, the boundaries between personal and professional use blur. While this flexibility can enhance productivity, it also introduces security challenges. Employees may not consistently adhere to security practices on their devices, potentially exposing sensitive company data to risks. One common human factor in this context is the use of unsecured Wi-Fi networks when working remotely. Employees may connect to public or unsecured networks, unwittingly exposing their devices and the organization's data to potential threats.

To address these challenges, organizations must implement clear BYOD policies and security controls. These policies should outline acceptable use, security requirements, and guidelines for personal device usage in work-related scenarios. Security controls may include the use of virtual private networks (VPNs), mobile device management (MDM) solutions, and encryption to safeguard data on personal devices. Furthermore, as the trend of remote work continues to grow, securing remote access and promoting secure practices among the workforce are essential elements of a robust cybersecurity strategy. Failure to address these human factors can lead to vulnerabilities that cybercriminals may exploit, potentially compromising an organization's data and security (Wani et al., 2020).

2.5.8 Employee Training and Education

According to (Triplett, 2022), employee training and education are critical human factors in cybersecurity. Effective training and education programs are essential for maintaining a vigilant and informed workforce. These programs should cover a wide range of topics, including emerging cybersecurity threats and best practices for mitigating them. Regular training sessions can help employees stay updated on the latest cyber threats and the methods cybercriminals use to exploit vulnerabilities. By increasing their awareness, employees are better equipped to recognize and respond to security threats appropriately. Additionally, cybersecurity training should include guidance on how to follow security policies, use security tools, and report suspicious activities. Training can also emphasize the importance of protecting sensitive data and the potential consequences of security breaches. Furthermore, the effectiveness of cybersecurity training and awareness programs can directly impact human factors in cybersecurity. Well-informed employees are more likely to follow security protocols and make informed decisions regarding cybersecurity. To conclude, employee training and education programs are indispensable in maintaining a vigilant workforce and minimizing the human-related vulnerabilities that can lead to security breaches (Dash & Ansari, 2022).

2.5.9 Crisis Response

Crisis response is a crucial human factor in cybersecurity. How employees respond to cybersecurity incidents can significantly influence the impact of a breach. Prompt reporting of security incidents is essential to quickly contain and mitigate potential damage. A well-defined incident response plan that outlines the steps to take in the event of a security breach is vital. This plan should include clear communication protocols to ensure that all relevant stakeholders are informed promptly. Effective crisis response can minimize the duration and scope of a cybersecurity incident, reducing its overall impact on the organization's security and reputation (Triplett, 2022).

2.5.10 Cultural and Organizational Factors

The culture and values within an organization can shape employee attitudes toward cybersecurity. An organization that prioritizes security and fosters a security-conscious culture is more likely to have employees who actively contribute to cybersecurity

Cultural and organizational factors play a significant role as human factors in cybersecurity. The culture and values within an organization can shape employee attitudes and behaviors regarding cybersecurity. An organization that prioritizes security and fosters a securityconscious culture is more likely to have employees who actively contribute to cybersecurity efforts. In such an environment, employees are more inclined to follow security policies and best practices, as they perceive security as a shared responsibility. A culture that encourages open communication about security concerns and provides resources for ongoing cybersecurity education can enhance the organization's overall security posture. Conversely, in organizations where cybersecurity is not a priority or where a lax attitude prevails, employees may be less motivated to adhere to security protocols, increasing the organization's vulnerability to cyber threats. Therefore, cultural and organizational factors are essential considerations in building a robust cybersecurity model, as they directly impact the human element of security within an organization (Jeong et al., 2019).

2.6 Impact of Human Factors in cyber security

A recent report highlighted that 83% of retailers in the United States are exposed to vulnerabilities, making them susceptible to cyberattacks (Kaur & Ram Kumar, 2022). These attackers often target customers' private data, which holds immense value in the e-commerce sector, where both business entities and customers become prime targets for cybercriminals and malicious activities (D'Adamo et al., 2021). Attackers employ various tactics such as data theft from online store databases, malware, ransomware, e-skimming,

distributed denial-ofservice attacks, and phishing attempts. This underscores the fact that as businesses increasingly embrace technology, including e-business and e-commerce, they gain opportunities but also face challenges like cybersecurity threats.

A security breaches survey conducted by the UK Government revealed a concerning trend: the number of security breaches had risen from 81% among large organizations to 90% (Solove & Hartzog, 2022). This highlights that security breaches are becoming more prevalent and are increasingly viewed as an expected element of contemporary business, one that cannot be eliminated. The report also emphasized the importance of businesses managing these risks effectively. Despite the implementation of staff awareness training programs, individuals continue to pose a significant threat, with human factors contributing to breaches as frequently as viruses and other forms of malicious software. As indicated in a study conducted by Solove and Hartzog (2022), a significant portion of breaches, amounting to 71%, stems from inadvertent errors made by employees, while an additional 68% result from employee negligence. As per findings by Dwivedi et al. in 2023, about 61% of breaches are the result of deliberate and malicious actions taken by individuals (Dwivedi et al., 2023).

In the current landscape, cybercriminals have shifted their focus from targeting machines to exploiting human vulnerabilities (Kaur & Ram Kumar, 2022). They seek to achieve their malicious objectives by taking advantage of end users' weaknesses. Therefore, human vulnerabilities represent a substantial threat to the security and integrity of computer systems and data. Human traits, such as the inclination to trust and assist others, as well as personal, social, and cultural characteristics, play a pivotal role in determining an individual's susceptibility to specific attack types and deception strategies (Papatsaroucha et al., 2021).

2.7 Existing Frameworks and Models for Human Vulnerability Assessment

This section reviews global and regional cybersecurity frameworks and human-vulnerability models, identifying their strengths, limitations, and applicability to MFIs. According to Grassegger and Nedbal (2021), most cybersecurity frameworks emphasize technical controls while under-addressing human-factor exposure. Nobles (2022) similarly notes that organizations tend to prioritize technology over human behavior, despite evidence that human weaknesses account for the majority of cyber incidents. This review responds directly to examiners' recommendations by expanding coverage beyond general frameworks to include models specifically addressing human vulnerabilities.

Table 2.1: Comparative Review of Existing Human Vulnerability Models and Frameworks

Framework/Model	Key Features	Limitations	Relevance to Study
NIST Cybersecurity Framework	Provides guidance on identifying, protecting, detecting, responding, and recovering from cyber threats.	Does not offer quantitative human-factor weighting; largely control-based.	Useful for structural alignment but insufficient for measuring human vulnerability.
ISO/IEC 27001	International standard specifying controls for information security management.	Focuses on governance and processes; lacks human-factor exposure metrics.	Provides foundation for hybridization in this study but cannot quantify vulnerability.
OWASP Top Ten	Prioritizes common application vulnerabilities.	Does not address human behavior or organizational practices.	Relevant for system security but not human vulnerability.
Human Factors Vulnerability Analysis (HFVA)	Emphasizes behavioral dimensions such as awareness and training.	Lacks empirical weighting and statistical validation.	Useful conceptual base but unsuitable for exposure computation.
Cyber Trust Index (CTI)	Measures organizational cyber trust and readiness.	Not specifically human-focused; qualitative scoring.	Partially relevant but does not provide exposure modeling.

The comparative matrix shows that existing frameworks emphasize governance, controls, and technical vulnerabilities, with limited attention to quantifying human-factor risks. This gap justifies the need for a model such as the CSHVEI, which empirically derives weights for human vulnerabilities using regression and factor-reduction techniques

2.8 Conceptual Framework

This section represented the variables used in the study. They can be classified as either Dependent, Independent, or Moderating Variables. The research investigated and explored on the major cyber security human factors vulnerabilities to determine their exposure index in an organization as proposed by (Lartey, 2021).

In this section, the conceptual framework guided the research and was presented in two stages; Stage one showed the Conceptual framework for the derivation of the formula for computing the Cyber Security Human Factor Exposure Index, and Stage two showed the CSHVEI Factor Reduction and stage three showed the Conceptual framework for implementation of the prototype.

2.8.1 Stage one: The derivation of the formula for computing the Cyber Security Human Factor Exposure Index

To increase comprehensiveness, improve accuracy, and enhance customization, this research proposed a hybrid human factor index model that blends insights from ISO 27001 and the NIST Cybersecurity Framework (CSF). This fosters a deeper understanding of an organization's human vulnerabilities, enabling the identification and mitigation of a broader range of security risks. Combining the two can leverage their respective strengths to achieve a more accurate and insightful assessment of human factors and organizational culture.

2.7.1.1 ISO 27001: 2022 and 2013

ISO 27001: 2022 and 2013 Annex A – Reference control objectives and controls that are used to guide the derivation of the formula for computing the CSHVEI.

A.5. Information security policies: These controls are the foundation of a strong ISMS, guiding policy implementation, communication, and review while establishing core security principles and commitments.

A.6. Organization of information security: Providing a comprehensive baseline for information security implementation and continuous operation, these controls establish its internal structure (roles, responsibilities) and address critical organizational aspects like project security integration, secure mobile device use, and secure teleworking practices.

A.7. Human resource security: The controls in this section aimed to ensure that those people who are under the organization’s control and can affect information security are fit for work and know their responsibilities and that any changes in employment conditions will not affect information security. It sets out controls for managing potential human vulnerabilities and promoting a strong security culture.

A.8. Asset management: Empowering responsible asset management, these controls identify key information assets, assign security responsibilities, and equip users with the knowledge to handle them based on classification levels.

A.9. Access control: The controls in this section aimed to limit access to information and information assets considering business needs, using formal processes to grant or revoke access rights. The controls consider either physical or logical access, as well as access made by people and information systems

A.11. Physical and environmental security: The controls in this section aimed to prevent unauthorized access to physical areas, as well as to protect equipment and facilities that if compromised, by human or natural intervention, could affect information assets or business operations.

A.12. Operations security: The controls in this section aimed to ensure that the operation of information processing facilities, including operating systems, are secure and protected against malware and data loss. Additionally, controls in this section required the means to record events and generate evidence, periodic verification of vulnerabilities, and the establishment of precautions to prevent audit activities from affecting operations.

A.16 &17. Information security incident and aspects of business continuity management: The controls in this section aimed to provide a framework to ensure the proper communication and handling of security events and incidents so that they can be resolved promptly and consider the preservation of evidence as required, as well as the improvement of processes to avoid recurrence and ensuring the continuity of information security management during adverse situations, as well as the availability of information systems.

2.7.1.2 NIST Cybersecurity Framework (CSF) Core Functions

Besides ISO 27001: 2022 and 2013 Annex A – Reference control objectives and controls this research will also use the NIST Cybersecurity Framework (CSF) core functions to guide the derivation of the formula for computing the CSHVEI. The functions and their key Categories considered relevant to this study are as follows;

GOVERN (GV) – Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy. The GOVERN Function is cross-cutting and provides outcomes to inform how an organization will achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization's broader enterprise risk management strategy. GOVERN directs an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles,

responsibilities, and authorities; policies, processes, and procedures; and the oversight of cybersecurity strategy.

IDENTIFY (ID) – Help determine the current cybersecurity risk to the organization. Understanding its assets (e.g., data, hardware, software, systems, facilities, services, people) and the related cybersecurity risks enables an organization to focus and prioritize its efforts in a manner consistent with its risk management strategy and the mission needs to be identified under GOVERN. This Function also includes the identification of improvements needed for the organization's policies, processes, procedures, and practices supporting cybersecurity risk management to inform efforts under all six Functions. In summary, it deals with;

(i) Asset Management: Inventorying and valuing organizational assets.
(ii) Business Environment: Understanding organizational dependencies and threat landscape.
(iii) Governance: Establishing cybersecurity policies, roles, and responsibilities.

PROTECT (PR) – Use safeguards to prevent or reduce cybersecurity risk. Once assets and risks are identified and prioritized, PROTECT supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events. Outcomes covered by this Function include awareness and training; data security; identity management, authentication, and access control; platform security (i.e., securing the hardware, software, and services of physical and virtual platforms); and the resilience of technology infrastructure. In summary, it deals with;

(i) Data Security: Protecting data at rest, in transit, and in use.
(ii) Access Control: Limiting access to authorized users and devices.
(iii) Security Architecture: Implementing secure technologies and configurations.

DETECT (DE) – Find and analyse possible cybersecurity attacks and compromises. DETECT enables timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse cybersecurity events that may indicate that cybersecurity attacks and incidents are occurring. In summary, it deals with;

(i) Anomalies and Events: Identifying and analyzing suspicious activity.
(ii) Security Continuous Monitoring: Implementing ongoing monitoring systems.
(iii) Detection Processes: Establishing procedures for investigating and reporting incidents

RESPOND (RS) – Take action regarding a detected cybersecurity incident. RESPOND supports the ability to contain the impact of cybersecurity incidents. Outcomes within this Function cover incident management, analysis, mitigation, reporting, and communication. In summary, it deals with;

(i) Incident Response: Containing, eradicating, and recovering from security incidents.

(ii) Mitigation Planning: Developing and practicing incident response plans.

(iii)Communications: Proactively communicating about cybersecurity incidents.

RECOVER (RC) – Restore assets and operations that were impacted by a cybersecurity incident. RECOVER supports the timely restoration of normal operations to reduce the impact of cybersecurity incidents and enable appropriate communication during recovery efforts. In summary, it deals with;

(i) Recovery Planning: Establishing procedures for restoring systems and data.

(ii) Improvements: Analyzing lessons learned and improving incident response capabilities.

(iii)Testing and Training: Validating recovery plans through exercises and training.

Table 2. 2: ISO 27001 Clauses

ISO 27001 clauses	**NIST CSF core Functions**	**CSHVEI variables**
A.5. Information security policies	GOVERN (GV) IDENTIFY (ID) PROTECT (PR)	Information security policies
A.6. Organization of information security	----------	Organization of Information Security
A.7. Human resource security	----------	Human Resource Security
A.8. Asset management	IDENTIFY (ID) GOVERN (GV) PROTECT (PR)	Asset Management

A.9. Access control	IDENTIFY (ID) PROTECT (PR)	Access Control
A.11. Physical and environmental security	PROTECT (PR)	Physical and Environmental Security
A.12. Operations Security	DETECT (DE)	Operations Security
A.16 &17. Information security incident and aspects of business continuity management	DETECT (DE) RESPOND (RS)	Information Security Incident aand Aspects of Business Continuity Management
----------	RECOVER (RC)	Recovery Planning

It is worth noting that the proposed combination of the selected framework and the standard not only captured comprehensive elements but also leveraged their underlying facets through tailored questionnaires, forming the model's foundation. By hybridizing, the proposed study intended to achieve two things: 1. Capture all the important clauses and core functions from the chosen guiding standard and framework, and 2. Leverage the deeper details within each element by designing specific questions around them, which ultimately form the basis of the mathematical model.

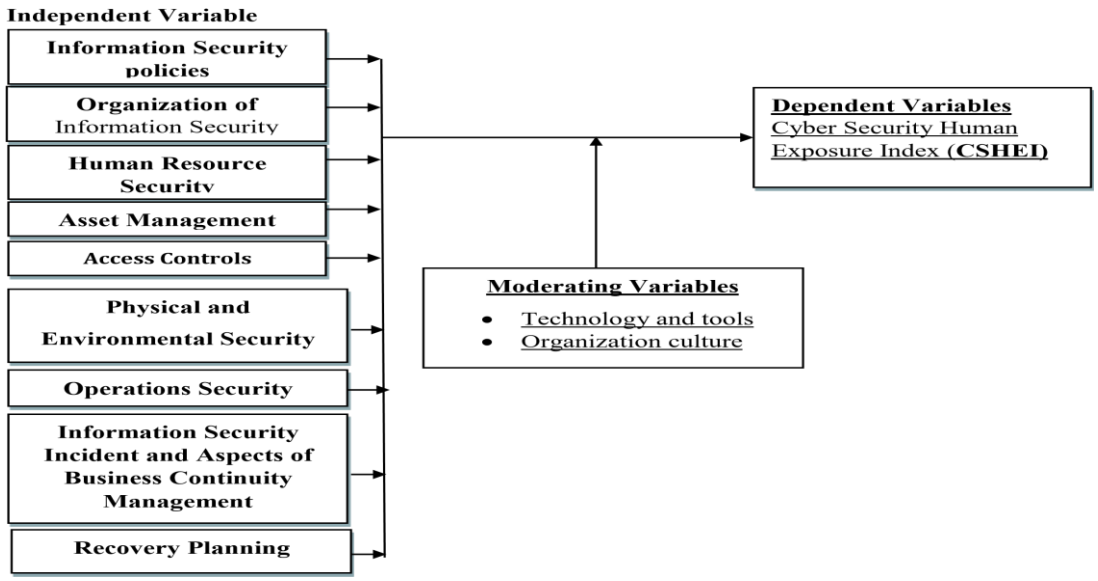


Figure 2. 3: Conceptual framework for the derivation of the formula

Source: (Koza, 2022; Paz, 2023)

2.8.2 Stage Two: CSHVEI Factor Reduction

To make simpler the conceptual framework, we condensed the CSHVEI variables into the following three categories based on the core principles of Human vulnerabilities that is; Human Errors, Ignorance, and Negligence:

i. **Human Errors**: These factors stand for inadvertent errors or oversights that may result in cybersecurity vulnerabilities. Operational errors, access violations, and improper handling of vital information are some of the common examples of human errors. The CSHVEI Variables reduced to human errors entails;
   - Operation Security which refers to Information system monitoring and security lapses
   - Access Control which refers to Errors in granting or overseeing authorization for users to access content.
   - Information Security Incidents: Errors in handling and reacting to security events Recovery Planning: Poor post-event response or post-event recovery plans.

ii. **Ignorance:** Lack of understanding, inadequate training, or knowledge gaps within the company are all related to ignorance. This can manifest in the misapplication or underapplication of key security practices and policies. The CSHVEI Variables reduced to human errors entails.
   - Information Security Policies: Poor understanding or implementation of security policies.
   - Organization of Information Security: Lack of awareness of the proper structuring and responsibilities of information security.
   - Human Resource Security: Insufficient training or awareness among personnel regarding their security responsibilities.

iii. **Negligence:** Negligence happens when important assets are not managed appropriately or when established security procedures are disregarded or broken. It frequently entails inadequate system, data, or physical environment security. The CSHVEI Variables reduced to human errors entails.
   - Asset Management: Improper handling and categorization of important assets.
   - Physical and Environmental Security: Negligence in securing physical settings that include vital systems or data.
   - Aspects of business continuity management that can result in Inadequate preparation for sustaining operations in the event of disruptions or security breaches

Below is a diagram showing how each CSHVEI variable flows into the three broad categories mapped into Human Errors, Ignorance, and Negligence to enhance simplified decision-making and better analysis. The benefit of this reduction is that it allowed a more focused assessment of security vulnerabilities and also helped in reducing noise in the data.

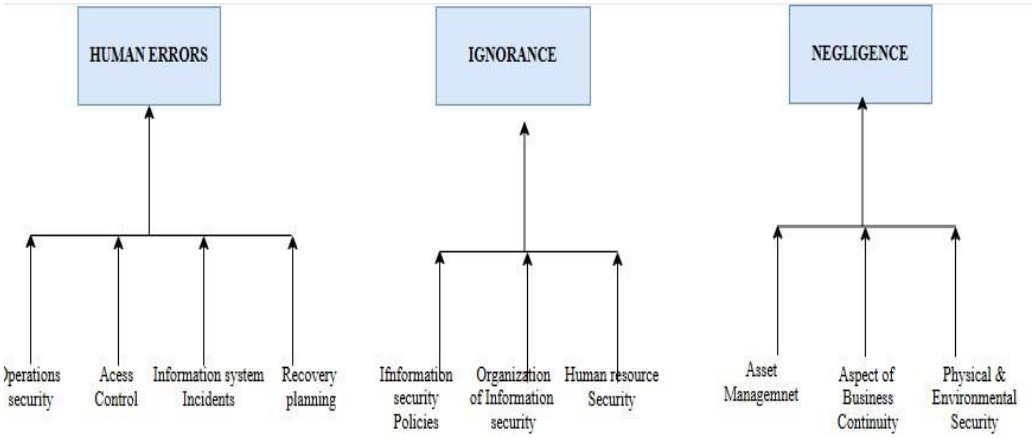


Figure 2. 4: **CSHVEI Factor Reduction**

Source: (Researcher, 2024)

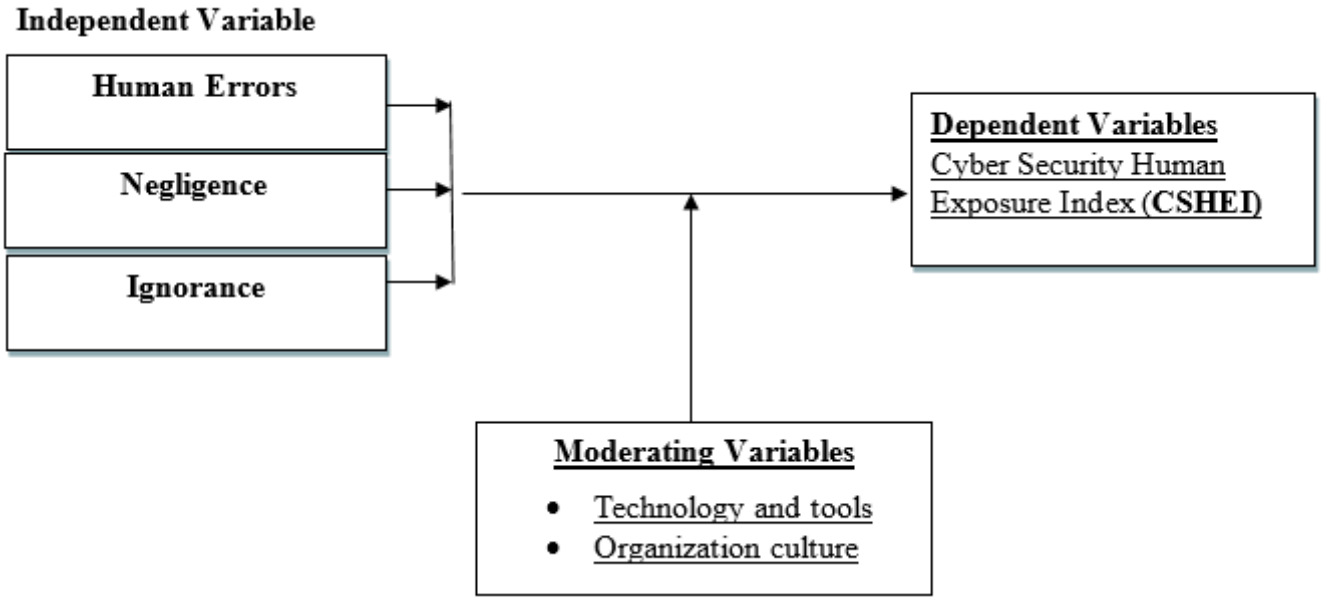


Figure 7 CSHVEI Factor Reduction Conceptual Framework

Source: (Researcher, 2024)

2.8.3 Stage Three: demonstration of how the prototype implementation will be done

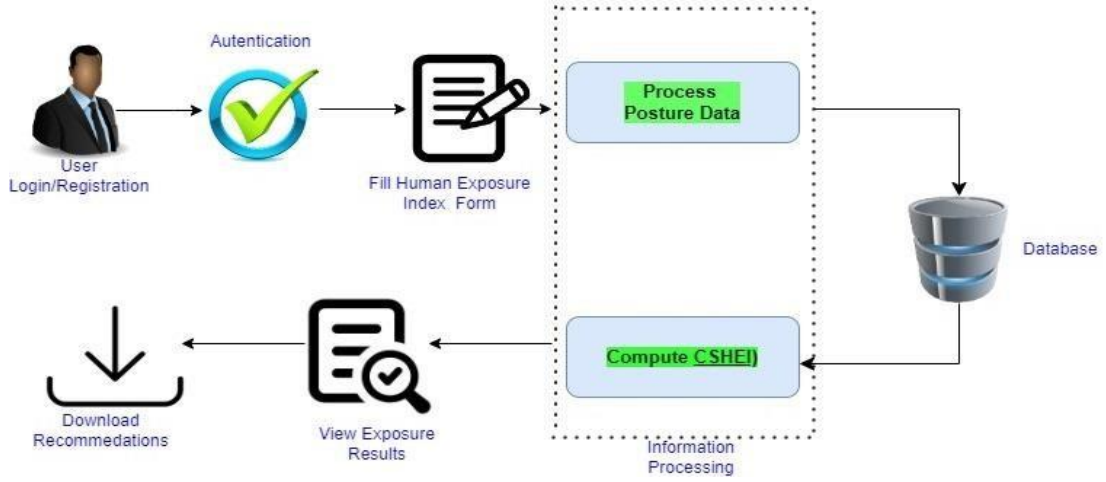


Figure 2. 5: **Conceptual Framework for implementation of a prototype**

Source: (Researcher, 2024)

The following modules were included in the prototype: a user authentication module that restricted access to authorized users only, a Posture input module that asked users to enter their best knowledge-based posture data, the information processing module that computed the CSHVEI using the stored weights and user-provided security posture information, while the record management module stores posture information and weights. The prototype also featured a module that showed CSHVEI data and offered a way to download CSHVEI data and relevant recommendations.

CHAPTER THREE

3. RESEARCH METHODOLOGY

3.1 Introduction

The research methodology adopted for this research study was presented in this chapter. The methodology presented included the target population, sample, sample size, sampling technique data collection, and analysis. The Development, implementation, and evaluation of the model are also covered in this chapter. This chapter concludes by outlining the ethical considerations that will direct the study.

3.2 An Integrative Literature Review (ILR) Methodology

Integrative review is a broad type of research review method that provides a broader summary of the literature and includes findings from a range of research designs(Sutton et al., 2019). It allows simultaneous inclusion of experimental and non-experimental research to more fully understand a phenomenon of concern. The purpose of this methodology was to identify and review secondary data relevant to the first objective of this study whose aim was to determine cyber security human factor vulnerabilities in organizations. The importance of this was to scrutinize and identify the cyber security human factor vulnerabilities in organizations, Subsequently, these would guide the design and implementation of a model that would determine the cyber security human factor exposure index model in organizations.

The Integrative literature review allows the researcher(s) to go beyond the analysis and synthesis of primary research conclusions and provides new insights and summarized knowledge about a specific topic (Gordon et al., 2020). The ILR allowed the inclusion of both secondary research studies, along with other documents including opinions, discussion papers, policy documents, and reports from focus groups. The review used databases to cover the most important papers and journals. Databases were used for the review to include the most significant papers and journals. The sources were searched based on the title, abstract, and keywords to review, critique, synthesize, and re-conceptualize the general notion of the cyber security human factor exposure index model in organizations and provide answers to the specified research questions.

3.3 Research Paradigm

According to a survey done by (Khatri, 2020), the Research paradigm is the theoretical or rather the philosophical ground for the research work. The research paradigm to be employed will be the positivist paradigm which shall be used (knowledge is revealed from

a neutral and measurable (quantifiable) observation of activity, action, or reaction) to quantify the human vulnerabilities during the implementation of the model.

3.4 Research Design

(Dutta, 2023) defines a research design as the roadmap, or blueprint a researcher uses as a guide for conducting a study. Typically, a research design is adopted by a researcher as a way of guiding how limited study resources are allocated. multiple-case study design and applied mixed-method research are the two main research designs that will be employed in this study for the collection of both qualitative and quantitative data. (Dawadi, 2021) contends that descriptive survey is important in studies that use both qualitative and quantitative data; thus, this study was placed well to adopt an Integrative literature search that was used to achieve the research objective i.e. *to determine cyber security human factor vulnerabilities in organizations.* The survey design was used to achieve research objective two i.e. *to Derive the cyber security human factor exposure index model in organizations.*

3.5 Population, sample size, and sampling Technique

3.5.1 Study Population

(Mweshi & Sakyi, 2020) defines a study population as the subjects or elements a researcher wishes to make inferences. Additionally, a study population is defined as the total collection of elements research would like to make inferences. This study targeted a total of 59 Microfinance Institutions in Nairobi County, Kenya. Table 3 show the distribution of the population.

Table 3. 1: Target Population

Category	Sample size
Management	59
IT	38
Customer Service	25
Operations	45
Total	**167**

Source: Registrar of companies (2024)

3.5.2 Sample size and sampling technique

Purposive sampling was used to target the financial institutions which were more vulnerable to cyber threats as per the latest research by Ross et al., (2023), where Chinese cyber spies subjected the mentioned offices through spear phishing. Sample on the other hand refers to

a segment or subset of the population that is selected for analysis. According to Lukman (2015), a sample size will be obtained using the following formula,

$$n = \frac{N}{(1 + Ne^2)}$$

Where; *n* =Representative sample *N*=population size *e*=Significance level 0.05 at 95% confidence interval

$$= \frac{59}{(1+59\times0.05^2)} = 52$$

The following Table show total number respondent distribution from the selected MFIs

Table 3. 2: Sample Size

Category	**Sample Size**
Management	52
IT	29
Customer Service	20
Operations	31
Total	132

According to the Table, the selected MFIs gave a total sample size of 132 respondents.

3.6 Data Collection and Analysis Methods

The study used both secondary and primary data. Primary data was collected using structured questionnaires with both open and closed questionnaires to seek clarification from the respondents. This was administered on a drop–and–pick basis. Secondary data was collected from the publication of private organizations, security policies, and regulatory authorities. The results of the study were examined using both descriptive and inferential analysis techniques. Specifically, Pearson chi-square test was computed to determine whether there exists a significance difference between groups. Furthermore, Spearman rank correlation was used to measure the significance of the relationship between independent and dependent variables. Finally, Multiple linear regression will be used to develop model weights. These methods were suitable because the researcher wanted to break down complex security issues into more manageable chunks.

3.7 Model development

The Cyber Security Human Vulnerability Exposure Index (CSHVEI) was computed as a function weight assigned to a human vulnerability as a mathematical model demonstrated by the formula shown below showing the coded variables

$$CSHVEI = W_1X_1 + W_2X_2 + W_3X_3 + e$$

Where;

W_1, W_2, W_3 …… W respectively are the *Various weights* computed using regression analysis on SPSS version.28

While;

$W_1X_1 + W_2X_2 + W_3X_3$ respectively are the coded *Human vulnerabilities* associated with cyber security human factors risks exposure as highlighted in the conceptual framework which entails; human errors, negligence and ignorance. e is the standard error of the estimate using regression analysis**.** The computation of **CSHVEI** will help in managing these parameters. Based on the analysed data collected from the 52 MFIs of Nairobi County, Different weights were assigned to the present posture of asset value which entails people, infrastructure, outsourced services, hardware, software, and electronic information. With this, the model now computes **CSHVEI** by comparing institutions' security posture against thresholds of ISO 27001 best practices and NIST core functions. Any results below the threshold meant that the institution's security status was threatening or wanting. In scenarios where the status was below the threshold, actions such as; Continuous Monitoring, Regular Risk Assessments, Employee Training, Patch Management, Incident Response Plan, Data Encryption, Multi-Factor Authentication (MFA), Vendor Management, Regular Security Training, and Drills, Security Audits and Penetration Testing, Regulatory Compliance, Executive Support and Cybersecurity Insurance were triggered.

3.8 Implementation of the Model

Proof of concept (PoC) is a certain method or idea being realized to demonstrate its feasibility or a demonstration in principle to verify that some concept or theory has practical potential (Walsh & Best, 2019).

3.8.1 Software development Lifecycle model

To implement this model, a rapid prototype was designed as the proof of concept. As defined by (Lauff et al., 2019), a prototype is a fundamental working model of a product or information system, usually built for demonstration purposes or something that will be further developed. In this study the model was in the form of a website to prove the

feasibility and also for managing the cyber security exposure risks within small and medium-sized financial institutions

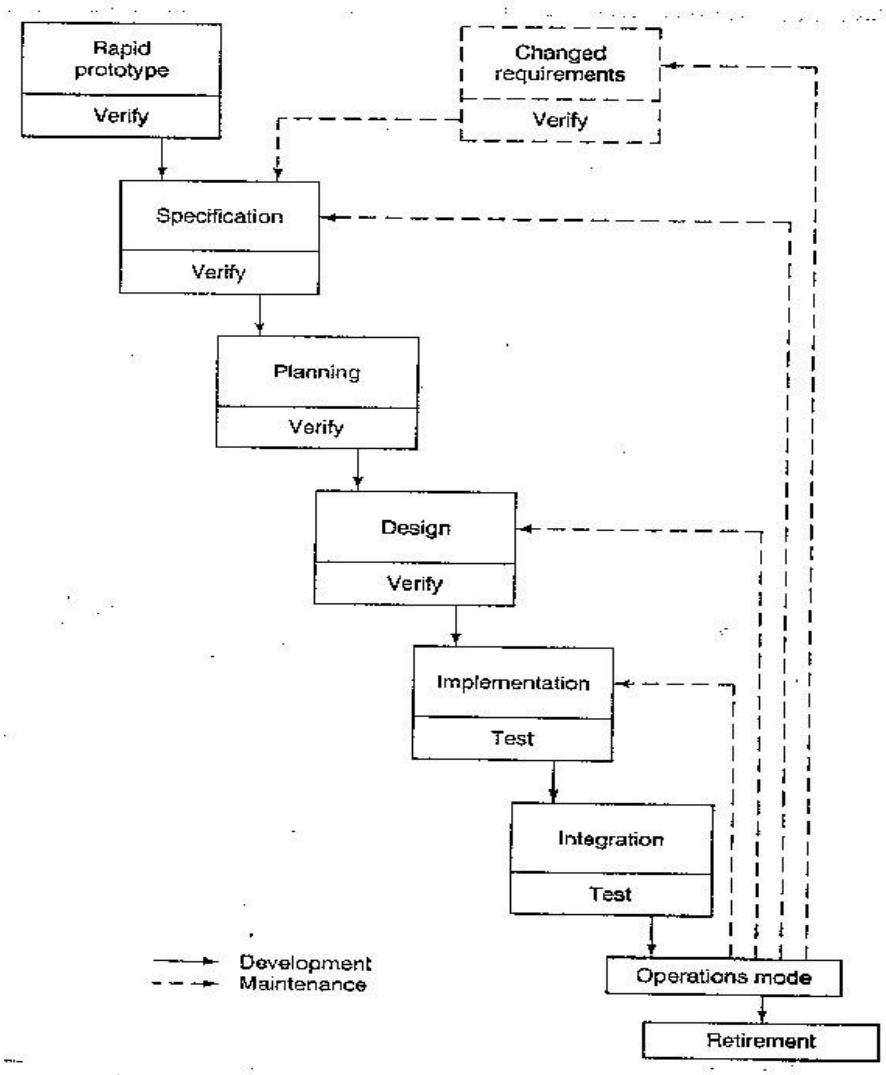


Figure 3. 1: **Rapid Prototype Model**

Source:(Jung et al., 2021)

3.8.2 Tools and equipment

To develop a robust and scalable web-based model to determine cyber security human vulnerabilities exposure index for organizations, we shall leverage various tools and technologies which entailed; Programming Languages like PHP which is for backend development, data processing, and machine learning. JavaScript for frontend development and interactivity. And HTML/CSS for building the user interface. MySQL which is an open-source relational database management system for storing structured data as the Database Management Systems.

3.9 Prototype Evaluation

According to (Alkhalil et al., 2020, p. 20), Prototype evaluation is a critical stage in the development process of a new product or solution. It is the stage where the model is tested to see if it matches the user's needs or preferences, one gets a chance to ask the target users for initial feedback on the design, usability, and user experience to identify strengths, weaknesses, and areas for improvement. The goal of prototype evaluation was to gather feedback from stakeholders, users, or experts to polish the prototype before moving forward with further development or production. Goal-based assessment approach, which is an evaluation approach for identifying the amount to which the prototype is meeting the overall predefined objectives, was used in this research to evaluate the prototype. (Ghoreishi & Happonen, 2020)

According to (Zhang et al., 2020), The Prototype evaluation will focus on the following

a. User Registration and Authentication Module:

Evaluation Objective: To evaluate the user registration and authentication process's efficiency, usability, and security.

Methods: Usability test and evaluate security. Offer participants the chance to sign up, log in, and reset their passwords. Gather information by observing how they interact.

Metrics include the success rate of login and registration, task completion times, user happiness ratings, and the detection of any security flaws.

b. Use poster input module

Evaluation Goal: Assess the posture input module's precision and usability.

Methods: Run usability tests with people entering different postures. Gather opinions on the module's usability and the precision of the posture capture.

Metrics: Time spent entering postures, the precision of posture identification, and user comments on the dependability and intuitiveness of the module.

c. Module for Record Management

Evaluation Objective: Ascertain the degree to which the posture information creation, storage, retrieval, and usage processes are facilitated by the record management module.

Method: To evaluate how simple it is to create, save, and retrieve posture records, employ user testing. Instruct participants in activities including adding

Metrics: Time taken to create and retrieve records, search success rate, user satisfaction with the organization, and accessibility of records.

d. Security Exposure Processing Module

Evaluation Objective: Evaluate the accuracy and effectiveness of the security exposure processing module in computing security exposure factors and comparing them with set thresholds.

Methods: Perform testing using both simulated and real-world data. Test the module's ability to accurately compute exposure factors and trigger alerts when thresholds are exceeded.

Metrics: Accuracy of exposure factor computation, correct identification of exposure threshold breaches, time taken to process exposure factors and system responsiveness.

3.10 Ethical Considerations

Several ethical considerations were adhered to during the gathering and model testing. This entailed assuring the respondents that the study was used for academic purposes only. Allowing respondents to participate voluntarily without pressure, informing respondents that they have the right to pull out any point during research, providing them with adequate information about the study before making and decision to participate, and finally assuring them that their privacy and confidentiality will be protected.

Some key ethical considerations entailed:

1. <u>Informed Consent:</u>

a. The goal, methods, risks, and benefits of the project must all be fully informed to the participants.
b. They should be able to participate voluntarily and intelligently.
c. It is important to record and obtain the consent voluntarily, free from coercion or manipulation.

2. <u>Confidentiality and Privacy:</u>

a. You must guarantee the confidentiality or anonymity of participant data as promised
b. Procedures for gathering and storing data should be safe and adhere to relevant privacy regulations.
c. Participants should have control over their data and be aware of how it will be shared and used.

3. <u>Avoiding Harm:</u>

a. Reduce any possible risks to participants' health and well-being.
b. Create protocols to handle any possible harm that might arise
c. Ascertain that participants can obtain resources and support when needed.

4. <u>Justice and Fairness:</u>

a. Select participants fairly and equally, avoiding biases.

b. Keep populations that are more vulnerable safe from abuse or unnecessary risk.
c. Ensure that the research benefits all participants and helps all participants.

5. Scientific Integrity:

a. Conduct research impartially and honestly, refraining from data fabrication or falsification.
b. Keep thorough and accurate records of all research methods and findings
c. Publish results responsibly and transparently, taking into account constraints and potential biases.

3.11 Summary of research methodology for each objective

Table 4 showed the summary of research methods for each research question. These included the research design, sampling strategy where applicable, relevant data, and data collection methods.

The research questions for the study were coded as below:

RQ1: What are the cyber security human factor vulnerabilities in cyber security?

RQ2: How can a cyber-security human factor exposure index model in organizations be derived?

RQ3: How can a cyber-security human factor exposure index model be implemented?

RQ4: How can the implemented model be verified and validated?

Table 3. 3: Summary of Research methodology for each objective

Research question	**Research design and methods**
RQ1	**Design:** mixed design using integrated literature review **Sampling strategy**: purposive sampling to select papers in a digital readiness assessment **Data to be collected:** human vulnerability factors **Data collection:** integrated literature search using key phrases from selected research databases **Data Analysis:** descriptive
RQ2	**Sampling strategy**: Stratified sampling **Data collection:** Survey questionnaires both online and physical **Data Analysis:** descriptive and inferential

RQ3	**Design:** Design science **SDLC:** RAD **Sampling**: Purposive sampling
RQ4	**Functional testing:** Alpha and beta testing with users **Data collection:** survey **Data analysis:** descriptive

CHAPTER FOUR

4. FINDINGS AND DATA ANALYSIS

4.1 Introduction

In research, data analysis is the process of analysing data and making inferences about a topic using logical and statistical methods. It is an essential component of research and is frequently employed to find trends, correlations, and patterns in the data. In this section, Response rate and respondents' demographics were analysed. Finally, descriptive and inferential analyses were utilized.

4.1.1 Response Rate

The proportion of respondents who conclude a survey out of all those invited is known as the response rate. It is sometimes referred to as the return rate or completion rate. Table 5 shows the distribution of response rate.

Table 4. 1: Response Rate

Sample size	Initial	Returned	Percent
Management	52	43	83
IT	29	25	86
Customer Service	20	16	80
Operations	31	28	90
Total	**132**	**112**	**85**

The study set to collect data with an initial sample of 132 respondents. After the administration of the instruments, 112 were duly returned. The overall response rate for the study is 85%. A high response rate indicates that the findings give a thorough and precise picture of the sampled audience. Sataloff and Vontela (2021) state that a response rate should ideally be above 60%; hence, the rate can be deemed satisfactory.

4.2 Demographic Data

The study aimed at analysing respondents' data relating to gender and department of operation.

4.2.1 Gender

The respondents' gender was analysed using both descriptive and quantitative statistics. Table 2 shows the findings.

Table 4. 2: Gender

	Frequency	Percent	Chi-Square	*df*	p-value
Male	55	49.1	0.036[a]	1	0.850
Female	57	50.9			
Total	**112**	**100.0**			

The analysis of gender indicated that 50.9% represented female while 49.1% were male participants. The chi-square statistic shows that there was no significant difference between male and female respondents (χ^2=0.036: p=0.850). This suggests that the sample was evenly distributed across the study population.

4.2.2 Department of Operation

An analysis of distribution of participants according to the department of operation was computed and results displayed in Table 3.

Table 4. 3: Department

	Frequency	Percent
Management	43	38.4
IT	25	22.3
Customer Service	16	14.3
Operations	28	25.0
Total	**112**	**100.0**

The analysis of departmental affiliation revealed that 38.4% of the participants were in management position. Those in operation and IT departments represented 25% and 22.3% respectively. Finally, those in customer service represented 14.3% of the sample.

4.3 Diagnostic Statistics

In combination with other forms of data analytics, diagnostic tests offer more profound insights into the data. The diagnostic tests that were utilized include, reliability and multicollinearity tests.

4.3.1 Reliability Tests

Cronbach's alpha was applied to evaluate the reliability of the instrument of data-collection. The level of internal consistency is assessed through this statistic by defining the extent to which a group of items is correlated with one another. It indicates the percentage of shared

variability amongst the items as a percentage of the total variability and thus indicates as to whether the items work well together in the measurement of the single underlying construct.

Table 4. 4: Reliability Test

Variable	No. of Item	Cronbach's Alpha	Decision
Human Errors	12	0.957	Reliable
Negligence	12	0.945	Reliable
Ignorance	12	0.935	Reliable
Cyber Security Human Exposure Index (CSHEI)	05	0.859	

According to the study, all the variables had Cronbach loading above the threshold of 0.7 coefficient. This suggests that the research instrument was reliable. According to Taber (2018), many studies commonly use 0.7 as the standard Cronbach's alpha value. The items are sufficiently consistent at this level and above to demonstrate the measure's dependability.

4.3.2 Multicollinearity

In regression modelling, multicollinearity is a condition that exists when two or more of the independent variables are substantially and highly linked thus making it hard to analyse the distinct feature held by each of the independent variables to the dependent variable. As a result, the process of estimation is consequently influenced in numerous ways such as through parameter estimation and inference.

Table 4. 5: **Coefficients[a] Model Collinearity Statistics**

		Tolerance	VIF
1	Human Errors	.224	4.471
	Negligence	.313	3.200
	Ignorance	.198	5.039

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

According to the table, all variables have Variance Inflation Factor below 10. It shows that there are no multicollinear symptoms in the model (Human Errors=4.471, Negligence=3.200 and Ignorance=5.039). According to Kim (2019) when both the condition number and the variance inflation factor (VIF) exceed 10, multicollinearity is considered to exist. Multicollinearity is an issue in the field of empirical research since it compromises the statistical standing of an independent variable. It is quite evident in the statistical literature that unstable and biased standard errors due to multicollinearity are the main problem of p-values that can also result in incoherent and unsustainable conclusions.

4.4 Descriptive Analysis

A collection of succinct descriptive coefficients that characterize a population as a whole or as a sample is known as descriptive statistics. A collection of succinct descriptive coefficients that characterize a population as a whole or as a sample is known as descriptive statistics. The analysis of data takes a central position in an empirical study. In the current debate, the focus involves the use of techniques that are termed as being descriptive given that they are only applicable to the quantitative aspect of observational data. The aim is to explain, visualize and generalize the applicable observations to a point where visible patterns occur fulfilling the demands of the data. The succeeding discourse sets out procedures that revolve around percentages, means, and standard deviations.

4.4.1 Cyber Security Human Exposure Index (CSHEI)

The main point of this investigation is the development of a statistical model that would be able to evaluate the Cyber Security Human Vulnerability Exposure Index in MFIs. The following are the findings of the study. Index of Human Vulnerabilities to Exposure to Cyber Security in MFIs: Descriptive Analysis of Dependent Variable

Table 4. 6: Cyber Security Human Exposure Index (CSHEI)

Statement	SD	D	N	A	SA
My company has put safeguards in place to lessen theft's possibility of phishing scams.	6%	23%	29%	20%	22%
Workers are aware of how crucial it is to confirm theft's legitimacy of people asking for private information	8%	27%	22%	26%	17%

Strong security measures are in place at my company to prevent unauthorized access to customer data	21%	15%	16%	33%	15%
In my company, employee data is handled with theft's same degree of security as client data	8%	23%	19%	26%	24%
Training has been provided by my organization and I know how to identify and report a DDOS attack	13%	21%	17%	31%	17%

Preventing phishing has grown crucial as more fraudsters use online scams to steal the personal data of unwary customers. In this study, 44 % confirmed that their company has implemented safeguards to lessen the possibility of phishing scams. Similarly, 43% of the participants agreed that workers are aware of how crucial it is to confirm the identity of people asking for private information. Following the solutions provided by the currently existing scholarly work, several steps of prevention can reduce chances of phishing attacks. According to Kessler et al., a composite strategy, namely, the concurrent use of automated mechanisms that include one-time passwords and multi-level barrier applications and specific behavioural modification, can help reduce the risk of successful victimisation significantly (Kessler et al., 2020). While many consumers are susceptible to phishing assaults, keeping up with the phishers' changing tactics is not an option.

Every company ought to strive to prevent unwanted access to client data. In this study, 48% of the participants affirmed that strong security measures are in place at my company to prevent unauthorized access to customer data. Correspondingly, 48% of the participants verified that training has been provided by their organization on how to identify and report a DDoS attack. Establishing robust password restrictions is a crucial first step in stopping unwanted access. This result is consistent with Kumar and Reddy's (2023) findings. who stated that frequent patch management and security upgrades guarantee that vulnerabilities are quickly fixed.

Establishing a security-conscious culture within the company requires educating staff members about cloud data security threats and recommended practices. By putting these safeguards in place, businesses may improve the security of their cloud environments and protect private information from unwanted access. Maintaining a strong cloud data security

posture in the face of changing threats requires constant monitoring, frequent updates, and staff training.

It is the duty of every individual within an organization to maintain compliance with data protection laws. In this study, 50% of the participants observed that in their company, employee data is handled with the same degree of security as client data. Data management initiatives may increase customers' concerns about security or actually make them vulnerable. As a result, caution must be used to guarantee that customer data is protected and utilized exclusively for its intended purpose. According to this result, which is consistent with that of Uddin et al. (2024), data protection in retail operations is essential in the era of digital transformation driven by data. Because the risks are ever-changing and unpredictable, businesses are always challenged by data breaches. The importance of dynamic capacity in improving security and comprehending the disruptive shifts of digital transformation cannot be overstated.

4.4.2 Human Errors

Human psychology is frequently seen as the most vulnerable link in the cybersecurity chain since it cannot be ignored in any cybersecurity scenario. Data was analysed through descriptive statistics. Table 7 displays results of the analysis.

Table 4. 7: Human Errors

Statement	SD	D	N	A	SA
How frequently do you double-check the accuracy of the information before sending or storing it?	6%	24%	22%	31%	16%
How often do you encounter accidental data entry errors in your daily tasks?	14%	9%	39%	21%	17%
How frequently do you find yourself accidentally deleting important files or data?	6%	23%	27%	21%	22%
How often do you find yourself accidentally sharing sensitive information (e.g., via email, or messaging platforms) with unauthorized persons?	7%	23%	24%	27%	19%
Have you ever accidentally compromised physical security by leaving doors unlocked, losing keys, or leaving sensitive areas unattended?	19%	17%	18%	34%	13%

How often do you accidentally share access credentials with unauthorized individuals (e.g., through email, messaging apps)?	16%	14%	19%	29%	21%
Have you ever mistakenly left your workstation or device unlocked when leaving your desk?	13%	20%	21%	24%	22%
How often do you find yourself making mistakes when handling the organization's assets?	14%	18%	26%	28%	14%
Have you ever mistakenly granted access to the wrong person or resource?	18%	16%	13%	38%	16%
How often do you encounter errors related to information security in your daily tasks?	21%	9%	25%	35%	10%
Have you ever shared confidential information with unauthorized individuals?	15%	21%	19%	33%	12%
Have you ever mistakenly deleted or modified important data that affected the recovery process?	19%	13%	22%	32%	13%

The importance of human aspects in information security cannot be overstated. In this study, 47% of the participants affirmed that they frequently do double-check the accuracy of the information before sending or storing it. However, up to 38% opined that they encounter accidental data entry errors in your daily tasks. Due to their heavy reliance on information systems (IS), organizations must manage the risks associated with these technologies. The results concur with those of Shouran et al. (2019), who stress that information security threats are a significant problem for many firms nowadays because they could have disastrous outcomes like financial damage, loss of credibility, and company liability. The success or failure of our attempts to protect and safeguard our companies, services, systems, and data is greatly influenced by the human element.

According to popular belief, human factors affect how people use information security technology. In this regard, 43% of the respondents affirmed that they frequently found themselves accidentally deleting important files or data. Moreover, 46% indicated that they frequently found themselves sharing sensitive information (e.g., via email, or messaging platforms) with unauthorized people. This perspective aligns with Joinson and van Steen (2018) who stress that cyber security is a "socio-technical" system that includes both human and technical components. It has been challenging to make progress based on this knowledge,

though. People have always been seen as the "weakest link" in cyber security, an unfixable system component that frequently thwarts information security experts' attempts to safeguard networks.

Human factors continually emerge as a key factor in having a successful cybersecurity. According to the empirical facts, 47 percent of the respondents acknowledged that they had a habit of compromising physical security like by leaving doors unlocked, losing keys, or forgetting to observe sensitive places. No less disturbing is the evidence of shareable credentials: 50 percent of respondents also reported sharing access information with unauthorized users through email or texting programs.

Based on these discoveries, practitioners ought to implement an integrated option of dealing with human error, including having a clear comprehension of the behavioural patterns, proposed changes, and the measures required to monitor the improvements. According to Stewart and Jurjens (2017), organizations do not follow simplistic compliance orders, but they get involved in a dynamic and multidimensional compliance system that incorporates legislature knowledge, integration of systems, and the identification and treatment of compliance gaps. The inferences of their findings are confirmed by the present study.

It is often acknowledged that user education and awareness are frequently the most effective factors in averting security problems. In this finding, it was observed that 46% of the participants indicated that they have ever mistakenly left their workstation or device unlocked when leaving their desk. Similarly, 42% acknowledged that they frequently found themselves making mistakes when handling the organization's assets. Human vulnerability is a defence flaw that users inadvertently cause. Therefore, it is possible for people to unintentionally forget, leak, or inadvertently divulge important information. It was noted that up to 54% of the participants affirmed that they have mistakenly granted access to the wrong person or resource. Similarly, 45% of the participants indicated that they often encounter errors related to information security in their daily tasks. In addition, 45% observed that they had shared confidential information with unauthorized individuals. Similarly, 45% of the participants avowed that they had mistakenly deleted or modified important data that affected the recovery process. This study's conclusion is in line with Grady's (2024) assertion that people are frequently thought of as the weakest link in the security chain. Eighty-five percent of data breaches are caused by human error or manipulation, according to the Verizon 2024 Data Breach Investigations Report. In order to give people, the information and abilities they need to recognize and address possible security risks, user education is therefore essential. By increasing knowledge and cultivating a culture that prioritizes security, businesses can

drastically lower the probability of successful assaults. In light of this, it is crucial to foster a culture of security in the current digital era by educating consumers on how to defend against online threats. In order to reduce risks, promote a cybersecurity culture, and adhere to legal obligations, user training is essential.

4.4.3 Negligence

Human errors represent a significant human factor in cybersecurity. This section focusses on negligence as the indicator of cyber security human exposure. Percentages were computed to examine patterns and trends among variables.

Table 4. 8: Negligence

Statement	SD	D	N	A	SA
How often do you bypass or ignore security protocols (e.g., using weak passwords, sharing login credentials) to save time or for convenience?	4%	29%	12%	37%	18%
How often do you leave your workstation unlocked or your computer unattended while logged into the system?	20%	10%	35%	16%	20%
How often do you leave your computer unattended without locking it?	15%	10%	23%	27%	25%
How regularly do you update your passwords as per the organization's policy?	8%	23%	20%	26%	23%
How often do you notice colleagues disregarding physical security protocols (e.g., tailgating, propping open doors)?	13%	22%	17%	32%	16%
Are Background Checks conducted on potential employees to assess their reliability and trustworthiness before hiring?	15%	21%	25%	22%	16%
Have you ever shared your work-related passwords with colleagues?	16%	20%	23%	34%	7%
Have you received training on how to manage access control (e.g., creating strong passwords, securing devices)?	15%	19%	21%	29%	15%

How frequently do you observe negligence or careless behaviour related to asset management among your colleagues?	18%	18%	19%	31%	14%
Do you consistently update your passwords or follow secure password practices?	19%	16%	21%	34%	10%
I leave my workstation without logging out of systems or devices.	20%	16%	16%	32%	16%
I do not regularly verify that my data backups are functioning properly.	20%	14%	17%	38%	11%

Organizations are thought to be unable to take the required precautions if they are unaware of possible hazards. The findings indicated that 55% of the respondents indicated that they bypass or ignore security protocols (e.g., using weak passwords, sharing login credentials) to save time or for convenience. In a similar view, 36% avowed that they leave their workstation unlocked or your computer unattended while logged into the system. These results are in line with Wu, Hanus, Xue, and Mahto's (2023) assertion that interpersonal communication and the media have an impact on people's ignorance of information security. Ignorance is more strongly shaped by personal characteristics, such as locus of control, intellectual curiosity, and computer fear. It was discovered that the belief that the Internet is a safe place is positively correlated with security ignorance.

Notably in recent years, cyberattacks have become more frequent, permanently altering the attack surface against organizations and consumers. In this regard, the results shows that 52% of the participants affirmed that they sometimes leave their computer unattended without locking it. This view was supported by 49% of the participants who confirmed that they sometimes update their passwords as per the organization's policy. This study supports that of Sangster (2020), who found that the majority of small and medium-sized businesses (SMBs) are utterly unprepared due to the rise in cybercrime that targets them. This is because they have been operating under the mistaken assumption that they are too small to be targeted by cybercrime. Instead, they believe they are too small to be seen, rather than too big to be failing. Because they think they are too tiny to be a target, many small to medium-sized businesses (SMBs) are unprepared for the growth in cybercrime.

Employees who lack the fundamentals of information security are said to render all security measures in a business ineffective. It was observed that 48% affirmed that they often notice colleagues disregarding physical security protocols (e.g., tailgating, propping open doors). In addition, 38% affirmed that there were some efforts to conduct background checks on potential employees to assess their reliability and trustworthiness before hiring. Ncubukezi (2022) claims that data manipulation occurs in businesses, which eventually results in data breaches. Data breaches are caused by denial-of-service attacks, data unavailability, illegal access, and compromised confidentiality, privacy, and integrity, even though some firms have implemented mitigating techniques. Both internal and external parties are responsible for these breaches in information security.

In empirical tests, it has always emerged clearly that the common occurrence of sharing passwords in an organisation significantly increases the ability of hackers to attack corporate networks. According to the present survey, 41 % of respondents share the passwords that are related to work with their colleagues on a regular basis. However, fewer people, only 34 %, reported that they have received training on how to manage access control effectively, including advice on how to create powerful password and cover the devices at certain intervals. These results confirm the findings of Calic et al. (2016) who note that human errors lying at the basis of cyber and network security include but are not confined to distribution of passwords, sharing too much personal information on social media, visiting suspicious websites, using prohibited external media, and clicking uncontrolled links, use of the same password on several accounts, opening attachments with suspicious sources, sending sensitive information via mobile networks, not securing personal electronic devices, and not updating software regularly.

In order to guarantee optimal security in any firm, it is essential to change the passwords every few months. According to 45% of participants, they underscored that they frequently observe negligence or careless behaviour related to asset management among your colleagues. Despite this observation, 44% reported that they often consistently update your passwords or follow secure password practices. This suggests that exchanging passwords is typically seen to be risky because most people use the same passwords across multiple websites, making it possible for others to access their other private data. This study is consistent with that of Whitty et al. (2015), who found that a common example of human cyber security failures is sharing passwords with friends, family, and even strangers. One of the most prevalent types of abuse among older adults is financial exploitation, which can result from sharing passwords.

It is evident that people and businesses are susceptible to disastrous outcomes in the absence of an appropriate data backup plan. The study established that 48% of participants reported that they leave their workstation without logging out of systems or devices. In a similar vein, 43% reported that they do not regularly verify that their data backups are functioning properly. A company is at risk if backups are not in place. The majority of transactions begin online, travel across various network devices, and end up on the appropriate servers. This finding is consistent with that of Rao, U.H., and Nayak, U. (2014), who found that individuals may not keep records of such transactions. Backups shield us from information security's availability and integrity threats. Only the backups can enable the availability of the associated systems in the event that the database becomes totally corrupted. Likewise, only the most recent backup allows us to restore the application to its previous state in the event that data integrity is compromised.

4.4.4 Ignorance

Human behaviour can either fortify or undermine cybersecurity. Employees' actions can open the door to vulnerabilities. This section deals with percentages of responses.

Table 4. 9: Ignorance

Statement	SD	D	N	A	SA
Does your organization offer sensitization programs on information security policies awareness?	8%	27%	22%	26%	17%
Do you know the proper procedures for reporting a security incident in your organization?	14%	18%	21%	28%	19%
Do you receive formal training on information security after every 12/18 months?	12%	23%	24%	27%	18%
Do you know the proper procedures for reporting a security incident in your organization?	13%	18%	23%	29%	17%
Are you aware of the procedures to follow in case of a physical security breach (e.g., unauthorized access, break-in)?	9%	22%	21%	26%	22%
How often do you refer to the organization's guidelines when performing tasks?	11%	18%	26%	25%	21%
Do you know how to identify potential risks or mistakes in your work before they become significant issues?	12%	20%	23%	21%	24%

Do you regularly update your passwords and follow the organization's guidelines for strong password creation?	9%	22%	26%	22%	21%
How often do you ignore or delay following up on security alerts or recommendations related to access control?	11%	17%	41%	21%	9%
How often do you or your colleagues seek guidance when unsure about asset management procedures?	12%	19%	22%	32%	15%
I prioritize my work over following strict security protocols.	7%	22%	23%	35%	13%
I am confident I can handle a security incident without needing formal recovery planning.	16%	13%	29%	21%	21%

Illegal entry can trigger system failure, reduce organisational efficiency, disrupt critical business in all sizes of business. Evidently, in a recently presented survey, 43 % of all the respondents report having received regularly sensitization programmes on information security policy awareness by their organizations. A similar percentage, that is, 47 %, respond that they are aware of the proper reporting approaches to security incident in their workplace. The results are in line with what Al-Daeef et al. (2017) suggest when they come to the conclusion that measures taken to provide security-based training should be focused on attracting the attention of the user, thus promoting the feeling of greater awareness and the ability to maintain the learned information in the long term. Security-awareness training is an invaluable tool to organisations wishing to protect sensitive data, limit the number of human-based security breaches, and mitigate the cost of incident response. The decreased likelihood of an attacker accessing corporate infrastructure can be achieved once the members of the staff are informed and prepared to act accordingly during the security crisis.

Employees in an organization requires formal information security training in order to reduce the risks associated with cybercrimes. In this study, 45% of participants indicated that they received formal training on information security after every 12 months. Furthermore, 23% indicated that they sometimes know the proper procedures for reporting a security incident in your organization. The current piece of work supports the observation made by Abawajy and Kim (2010) that increased information security awareness and training are essential in eliminating information security risks arising out of human-related vulnerabilities. This training can be implemented in various delivery channels and promises a great potential in increasing the awareness of the users and limiting the harmful consequences of their behaviours and mistakes, which is an objective that cannot be achieved using only purely

technical mitigation measures. The primary objective of any security training program should be to help users retain the knowledge they have learned for a long time so they can apply it to other security-related disciplines. The effectiveness of the suggested user training techniques varies, as do the implementation processes.

Short, intense training in cybersecurity combined with knowledge of the policies and procedures of the organization with regard to cybersecurity is an invaluable addition to the overall design of a holistic cybersecurity strategy. During the current study, 48 % of the respondents answered that they were aware of the prescribed action to follow in case of any physical security breach (e.g., unauthorized access or break-in). Similarly, 26 % responded saying that they sometimes used organizational guidelines in carrying out routine jobs. Amankwa et al. (2014) carried out a conceptual investigation on the issue of information security awareness, training and education to establish the existence of disparities. The results of this investigation were useful to organizations in determining the times when security awareness programs were the suitable intervention and when formal training or instruction became the suitable intervention to offer to facilitate improvement of personnel.

Security awareness training for system and application users is crucial to reducing risk to the IT systems. The study established that 45% affirmed that they have knowledge on how to identify potential risks or mistakes in your work before they become significant issues. Similar findings were propounded by 47% of those who reiterated that they regularly update their passwords and follow the organization’s guidelines for strong password creation. In a survey on the organizational information security climate, Kessler et al. (2020) looked into the attitudes and behaviours of staff members. The findings show that a safe workplace does have a positive impact on employee behaviour, which lowers the frequency of data breaches. The authors concluded that enhancing cybersecurity requires personnel training. According to the same study's findings, older workers handled private and sensitive material with greater caution than their younger counterparts.

One of the most significant cybersecurity issues facing businesses of all sizes is unauthorized access. According to the finding, 41% asserted that they often ignore or delay following up on security alerts or recommendations related to access control. A similar view was advocated by 47% of those who stated that they sometimes seek guidance when unsure about asset management procedures. Similarly, 37% of participants affirmed that they prioritize their work over following strict security protocols. Finally, only 43% reported that they were confident that they could handle a security incident without needing formal recovery planning. Ahola, M. (2019) highlights that although cyberattacks are typically blamed for data breaches,

physical threats can equally affect enterprises. If unauthorized individuals manage to get access to secure premises, they may steal or view credentials and confidential information. A sensible mitigation strategy needs to be aimed at systematically minimizing the likelihood of a mistake by altering work techniques, practices, and technologies.

4.5 Spearman Rank Correlation Analysis

Spearman R correlation coefficient is a calculative measure that monitors the size and direction of the association that exists between two nominative variables, or ρ, which is also represented by r_s. Table 10 shows the findings of these correlations between independent and dependent variables

Table 4. 10 Correlations Matrix

			CSHEI	Human Errors	Negligence	Ignorance
Spearman's rho	**Cyber Security Human Exposure Index (CSHEI)**	Correlation Coefficient	1.000			
		Sig. (2-tailed)	.			
		N	112			
	Human Errors	Correlation Coefficient	.654**	1.000		
		Sig. (2-tailed)	.000	.		
		N	112	112		
	Negligence	Correlation Coefficient	.818**	.601**	1.000	
		Sig. (2-tailed)	.000	.000	.	
		N	112	112	112	
	Ignorance	Correlation Coefficient	.831**	.668**	.702**	1.000
		Sig. (2-tailed)	.000	.000	.000	.
		N	112	112	112	112

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

According to the findings, there is a statistically significant relationship between human errors and cyber security human exposure index (rs=0.654;p=0.000).This implies that as human errors continue to surge, organizations cyber security human exposure index increases.

Secondly, there was evidence of a significant relationship between negligence and cyber security human exposure index (rs=0.818;p=0.000).This means that generally, human

errorrelated data breaches are frequently caused by employees' careless behaviour or poor judgment.

Finally, ignorance significantly correlates with cyber security human exposure index (rs=0.831;p=0.000).This suggests that these unintentional ignorance-based actions allow cybercriminals to run harmful malware.

4.6 Regression Analysis

Regression analysis is a valid statistical method that allows conducting thorough research on the correlations between two or more variables. Multiple linear regression is used in the discussion at hand.

4.6.1 Summary Table

The description of model characters, R, R-Square, adjusted r-square, and standard error, is articulated below.

Table 4. 11: Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.951[a]	.905	.902	.32341

a. Predictors: (Constant), Ignorance, Negligence, Human Errors

b. Dependent Variable: Cyber Security Human Exposure Index (CSHEI)

The model summary shows that 90.2 % in Cyber Security Human Exposure Index (CSHEI) 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.

4.6.2 ANOVA

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

Table 4. 12: ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	107.055	3	35.685	341.184	.000[b]
	Residual	11.296	108	.105		
	Total	118.351	111			

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

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 (CSHEI), F (3,108) =341.184, $p<0.05$, Adjst. R square=0.902.

4.6.3 Coefficients

Multiple linear regression was used as the analysis methodology in the current study. The major goal of this regression method is to establish how much an independent variable has influence on a dependent variable. Thereby, regression coefficients are estimated and interpreted as the weights of the model.

Table 4. 13: Coefficients[a]

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
	B	Std. Error	Beta			Tolerance	VIF
1 (Constant)	-.062	.110		-.562	.576		
Human Errors	.167	.061	.172	2.729	.007	.224	4.471
Negligence	.539	.053	.539	10.128	.000	.313	3.200
Ignorance	.324	.072	.298	4.472	.000	.198	5.039

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

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

4.6.4 Model Equation

The model equation was thus developed as:

$Y= \alpha + B1x1 + B2x2 + B3x3 + e$

CSHEI = -0.062+(0.167*H. E) +(0.539*N. G) +(0.324*I. G) + 0.32

Key

α=constant

H. E= human errors

N. G= negligence

I.G=Ignorance.

4.6.5 Limitations of Statistical Inference

Although statistical inference provides valuable insights into the relationships among variables in this study, several limitations should be acknowledged to ensure proper interpretation of the results.

a) Potential Bias in Responses

Self-reported data may introduce social desirability bias, recall bias, or respondent misunderstanding, which can affect the accuracy of parameter estimates. Even with high reliability coefficients, subjective perceptions may not perfectly reflect actual behaviors or vulnerabilities.

b) Limited Generalizability

The study focuses on MFIs within Nairobi County; therefore, the findings may not fully generalize to MFIs in other counties or financial sectors with different technological infrastructures, cybersecurity policies, or user cultures. Statistical inference assumes representativeness of the sample, but real-world variations may limit external validity.

c) Assumptions of Regression Analysis

Multiple linear regression relies on assumptions such as linearity, normal distribution of residuals, homoscedasticity, and absence of multicollinearity. Although diagnostics were performed to check these assumptions, minor deviations can still influence coefficient accuracy and interpretation.

d) Sampling Limitations

The use of purposive sampling for institutions and stratified sampling for respondents improves relevance but may reduce randomness. This may lead to sampling bias, limiting the broader applicability of the inferred results.

e) Temporal Limitations

The study captures data at a single point in time. However, cybersecurity behaviors and threats evolve rapidly. Thus, statistical relationships identified may shift over time, limiting longitudinal generalizability.

f) Model Specification Error

Statistical inference is constrained by the variables included in the model. Although human error, negligence, and ignorance were grounded in theory and factor analysis, unobserved variables may influence cybersecurity vulnerabilities and create omitted-variable bias.

CHAPTER FIVE

5. SYSTEM IMPLEMENTATION

5.1 Introduction

This chapter presents how the model for determining human vulnerability index for microfinance Institutions (MFIs was implemented. Section 5.2 states the purpose for which the model was implemented while section 5.3 offers an overview of the design process. Section 5.4 provides an overview of the system engineering and design processes, while sections 5.5, 5.6, and 5.7 discuss the evaluation, model security, and potential areas for further improvement of the model, respectively.

5.2 Purpose of the Model

This research purposed to determine the cyber security human vulnerability exposure index of the MFIs. In alignment with the fourth research question, the model was implemented to offer an automated and streamlined approach for assessing the human vulnerability index of MFI as a web-based application.

5.3 System Functional Overview

The model was anticipated to support MFI user registration, MFI user logins, perform human vulnerability assessment and evaluation, and produce recommendations reports from user scores that went below the threshold. Recommendations herein are the needed measures for MFI to mitigate human vulnerability and improve the overall security posture of the organization.

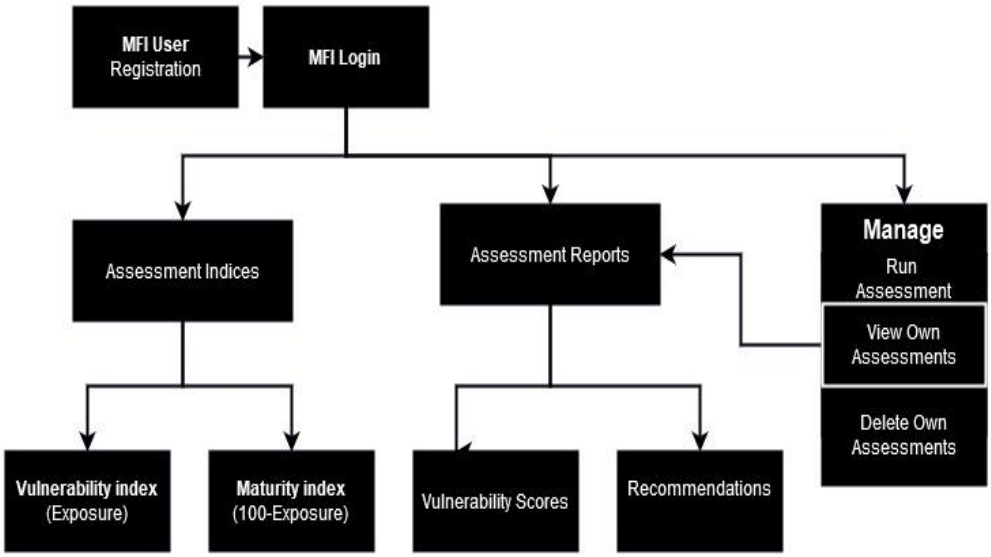
5.4 Software Design

The design process of the MFI human vulnerability index assessment system was done through the conventional stages of software engineering and design processes which includes the following stages; Requirement Analysis, High-Level Design (HLD), Low-Level Design (LLD), Implementation, Testing and Validation, and Maintenance. The following section presents the details of the activities that were carried out in each stage of the design process:

(i) Requirements Analysis: The purpose of this stage was to understand what the software needed to do in form of functional and non-functional requirements and use cases. As such there was need to design the MFI user portal that was separate from the admin portal. The decision of tools for implementation was done at this stage and involved PHP, MySQL, Bootstrap 4, JavaScript, JQuery and Ajax

because of the low cost of implementation, efficiency and the fast community of users.

(ii) High-Level Design (HLD): The overall architecture and design of the MFI human vulnerability system was curated at this stage. All modules, components and integrations were ideated and appropriate technologies for each was selected. These designs were summarized as presented in the flow diagram in Fig 10 below.



: MFI User Portal Flow Diagram

Source: Researcher (2024)

(iii) Low-Level Design (LLD): The main focus of this stage was to create a detailed design of each module and component by defining data structures, algorithms and logic for each component of the system. As such, data flows between components, interfaces and, logic, abstraction and algorithms were specified as presented in the flowchart in section 5.5.

(iv) Implementation: The design was translated into executable PHP, JQuery, Bootstrap and SQL codes. The implementation adopted rapid application development as the appropriate methodology. The executed codes produced interfaces presented in section 5.3

(v) Testing and Validation: The purpose of this stage is to ascertain that the software satisfies design requirements and functions as expected. As a result, objective-based or goal-based assessment was used to assess the system. This required the designer to evaluate some software components against preset requirements. This was done

to ensure that the codes for various components and modules were compatible. The results of the evaluation are presented in table 17 below.

5.5 System Implementation

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 following sections present different modules developed through for the model;

5.5.1 Registration Module

The module allows the 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 11 below. 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. Figures 11 and 12 below presents registration module and flow chart of the MFI user registration respectively.

Figure 5. 1: **User Registration**

Form Source: Researcher (2024)

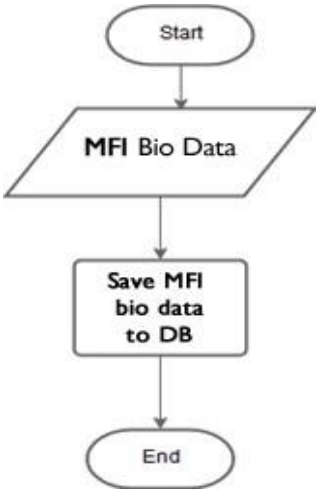


Figure 5. 2: **Registration Flowchart**

Source: Researcher (2024)

5.5.2 Login Module

This module controls the access to the system by ensuring that only registered and authorized MFI users access user portal while authorized admins can access the admin portal. Authenticated users and admins can therefore carry out various activities within the system after they successfully login. MFI users can use either username or email with correct passwords to improve usability and convenience of the authentication process. The model further checks whether the user is activated or not. The user is inactive by default when they register and can only be active when the admin activates them at the admin portal. In addition, this module is in charge of managing user sessions, which are created after a user log in successfully and terminated upon logout.

In summary, the login process checks the user database to confirm that the provided email address or username exists and that the entered password matches its stored, decrypted equivalent. If the system cannot find a matching email or username, it notifies the user that no such account exists. Likewise, if the password does not correspond to the stored value, an error message is displayed indicating an incorrect password. In both situations whether for user or

administrator accounts—the system redirects back to the login screen, as illustrated in Figures 14, 15, and 16 through the associated flowchart and interface designs.

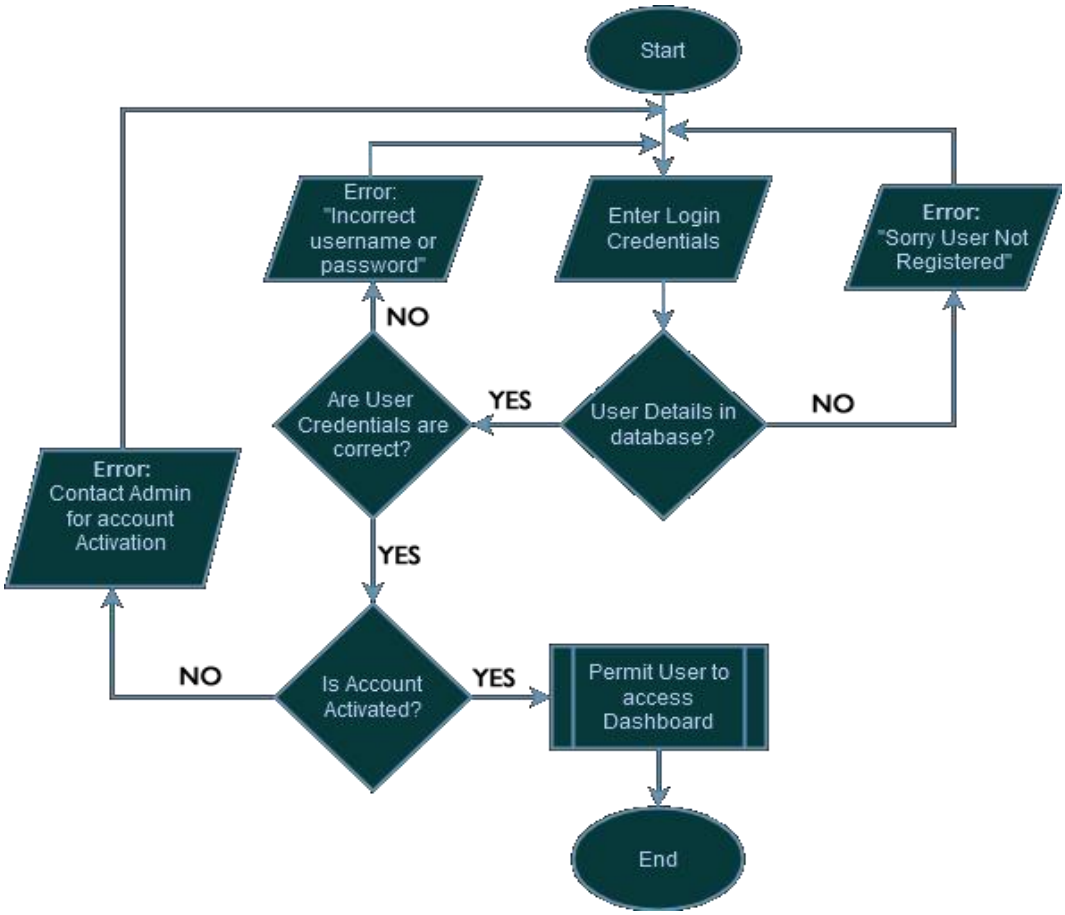


Figure 13: Login

Flowchart Source:

Researcher (2024)

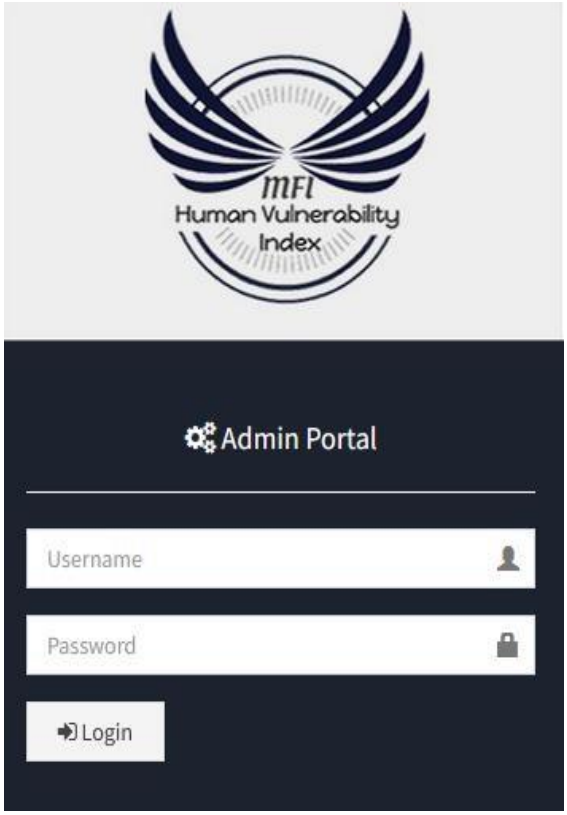


Table 4. 14: MFI User Login

Source: Researcher (2024)

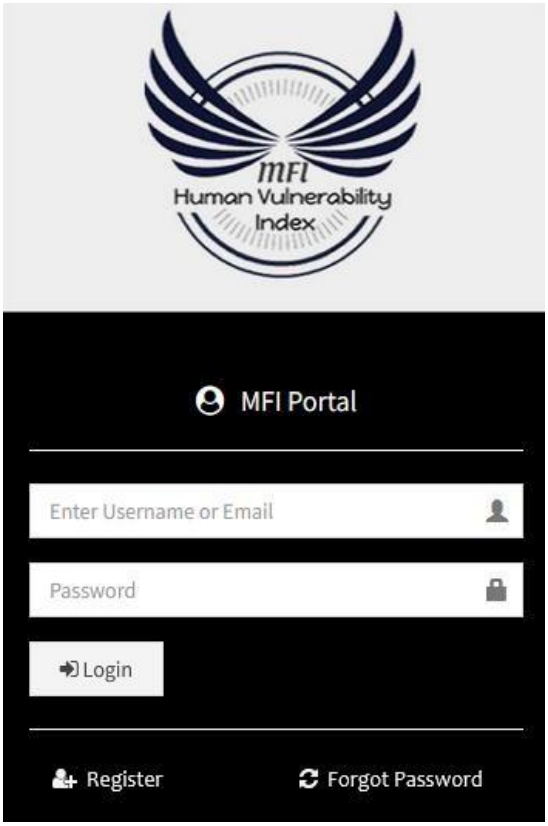


Table 4. 15: MFI Admin Login

Source: Researcher (2024)

5.5.3 MFI User 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.

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. The figures 16 and 17 below shows the MFI user dashboard and admin dashboard respectively.

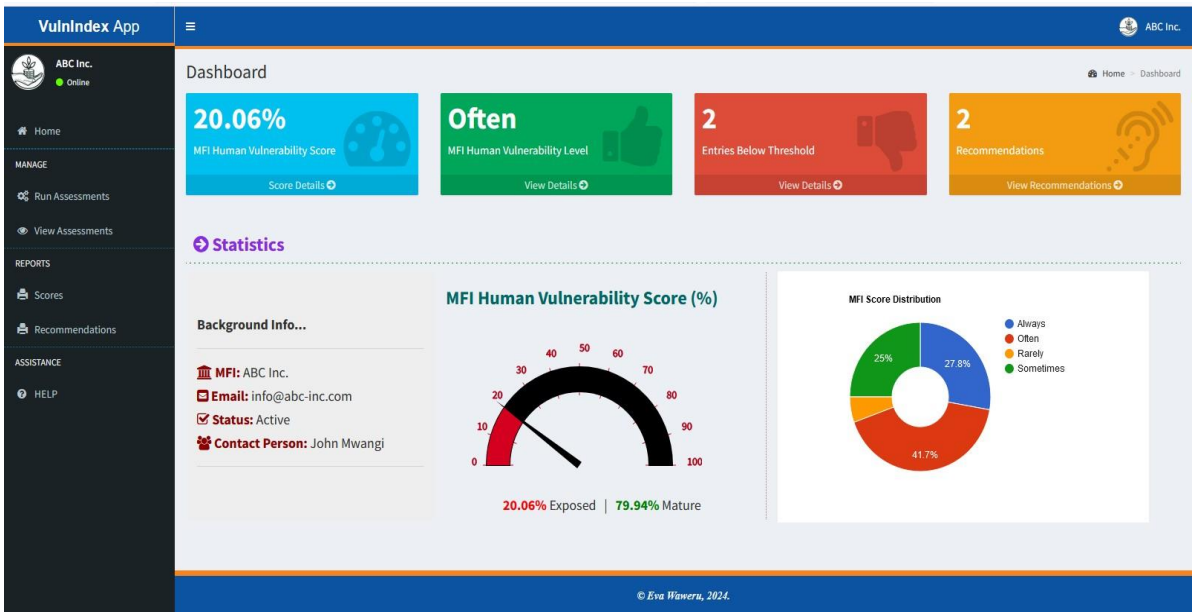


Figure 16: MFI User Dashboard

Source: Researcher (2024)

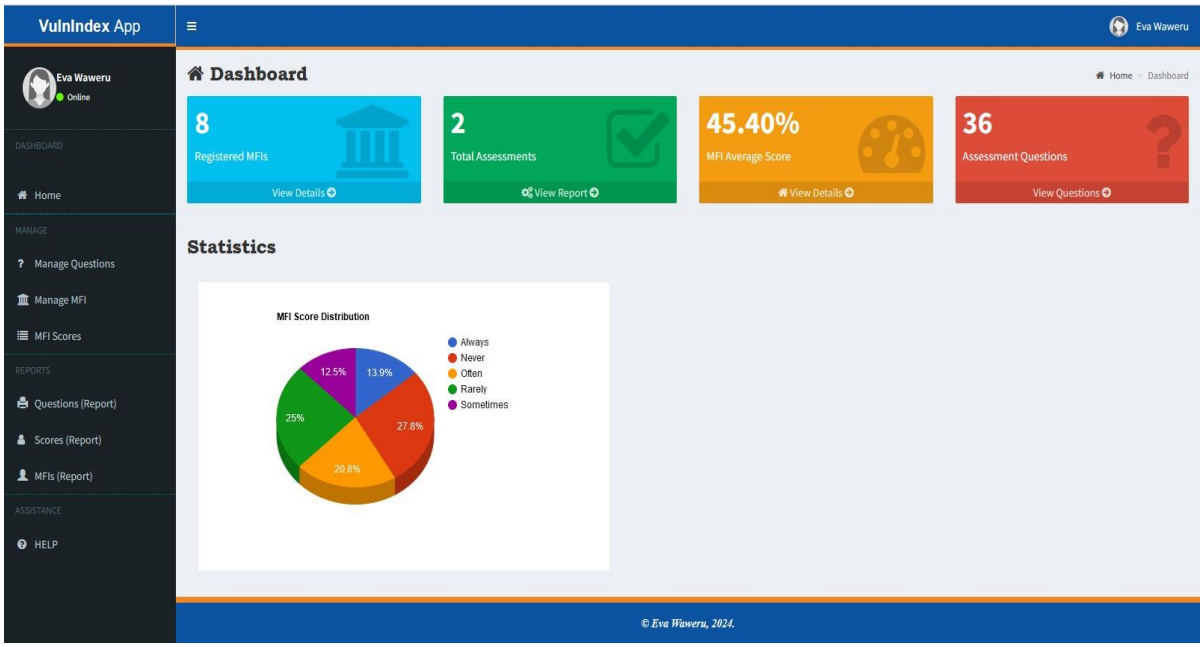


Table 4. 16: **Admin Dashboard (2024)**

Source: Researcher (2024)

5.5.4 Navigation Menu

Users can effortlessly navigate the system because to its features. Easy navigation was ensured by the use of side menus for both MFI users and admins. The following figures 18 and 19 display MFI User sides menu and admin side menu respectively.

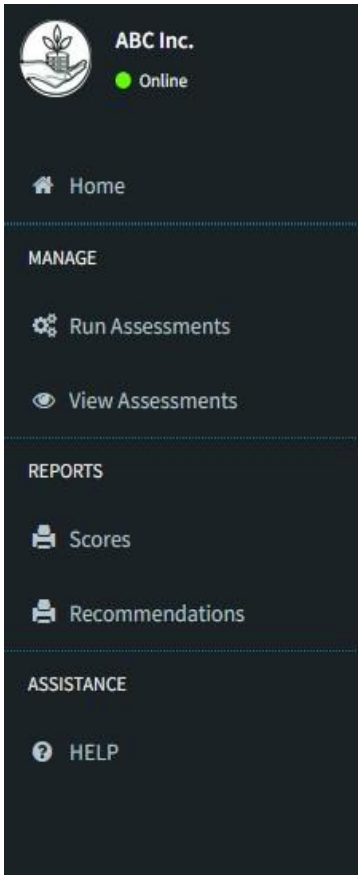


Figure 18: MFI User Menu

Source: Researcher (2024)

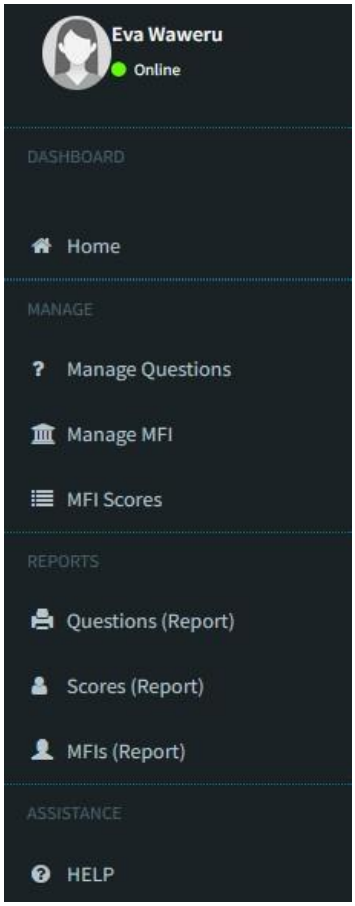
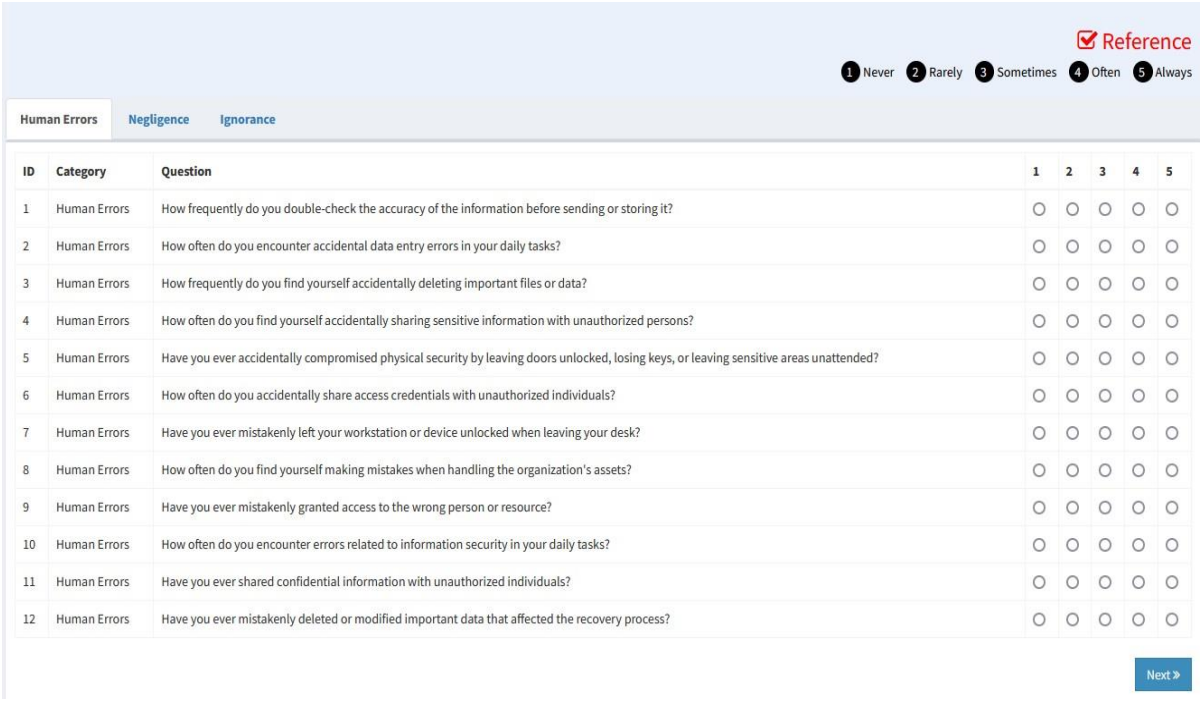


Figure 19: Admin Menu

Source: Researcher (2024)

5.5.5 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 20 below shows the graphical user interface for the human vulnerability assessment module, and Figure 21 shows the flowchart for the human vulnerability assessment procedure.



Reference

1 Never 2 Rarely 3 Sometimes 4 Often 5 Always

Human Errors | Negligence | Ignorance

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?	○	○	○	○	○

Next »

Figure 5. 3:Human Vulnerability

Assessments Page Source: Researcher (2024)

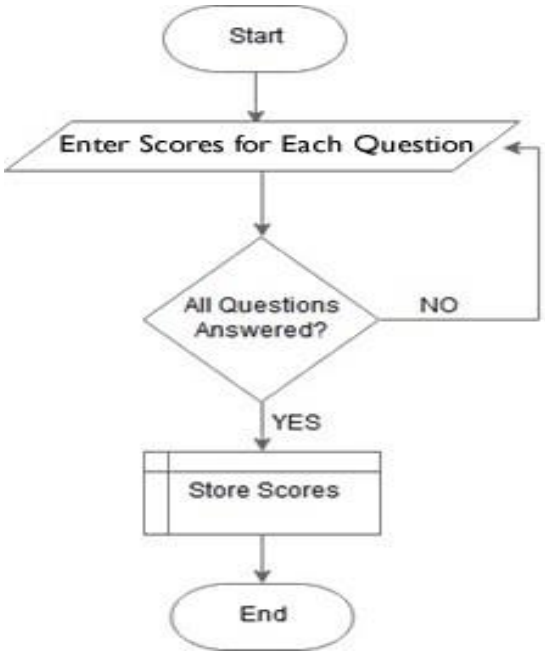


Figure 5. 4:Human Vulnerability Assessment Flowchart

Source: Researcher (2024)

5.5.6 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 22 and the human vulnerability and maturity gauge is presented in figure 23.

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

CSHEI = -0.062+(0.167*H. E) +(0.539*N. G) +(0.324*I. G) + 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 5. 5. Human Vulnerability Index Computation Code

Source: Researcher (2024)

Figure 5. 6: **Human vulnerability Index Gauge**

Source: Researcher (2024)

5.5.7 MFI Score Distribution

This is a section of the dashboard display that gives the MFI user a quick view of score distribution of for responses that the user gives for human vulnerability assessment questions.

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 24 below.

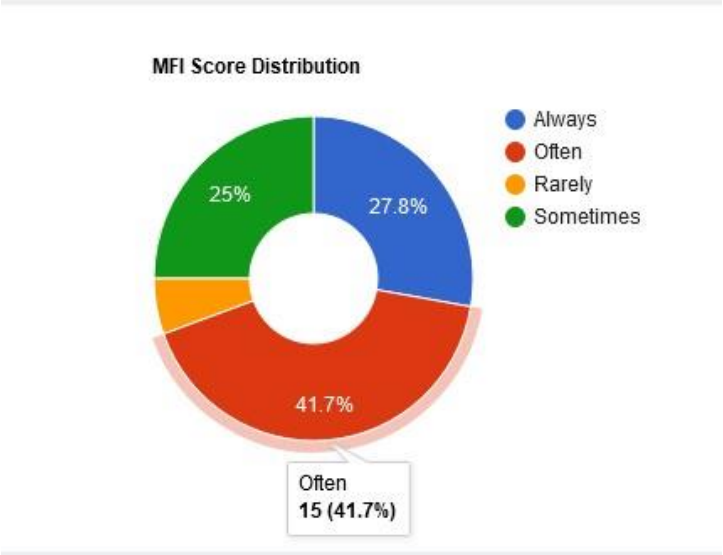


Figure 5. 7: **MFI Score Distribution Chart**

Source: Researcher (2024)

5.5.8 Assessment Questions Setup

The system is scalable by the fact that it allows for addition, updates or removal of assessment questions when there is need to do so. This feature is a reserve for the system admins through assessment questions module shown in Fig 25 below.

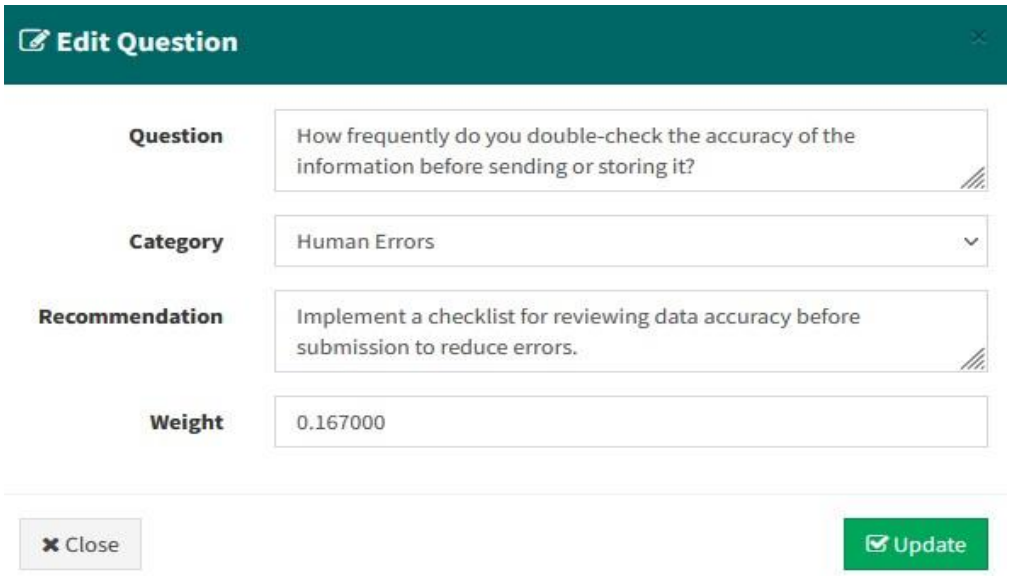


Figure 5. 8: **Human Vulnerability Assessment Page Source:**

Researcher (2024)

5.5.9 Human Vulnerability Index Calibration

The model prompts responses from MFI users who scores keys in the responses to varied assessment questions in a scale of 1 to 5 where 1 represents Never, 2 Rarely, 3 Sometimes, 4 Often, and 5 Always. As such, the calibration of the system ranges from the worst case when the user responds by keying in 1 for all the questions to imply that they Never did according to the requirements of the assessment question.

This translates to a score of 79.67% exposure index or 20.33% maturity index as indicated in figure 26 below. The metrics doesn't start from zero simply because the Likert scale begins at a least score of 1 and not 0. This therefore imply that the lowest score of maturity has the highest score index of exposure, that is; The model as an instrument can possibly measure human vulnerability index of MFI 0.2033 and 1 or, put in other words, 20.33 percent to 100 percent. This is referred to as a possible case. The other area of the scale between 0 and 0.2033 cannot be measured and therefore referred to as the impossible state.

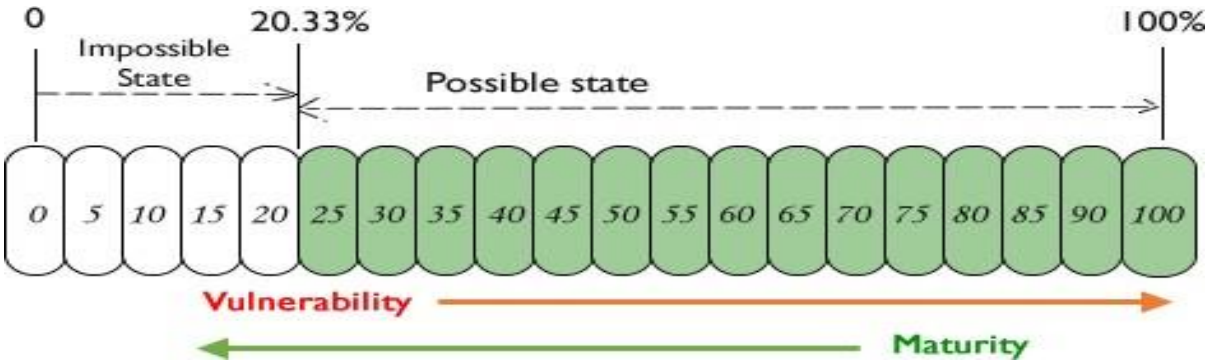
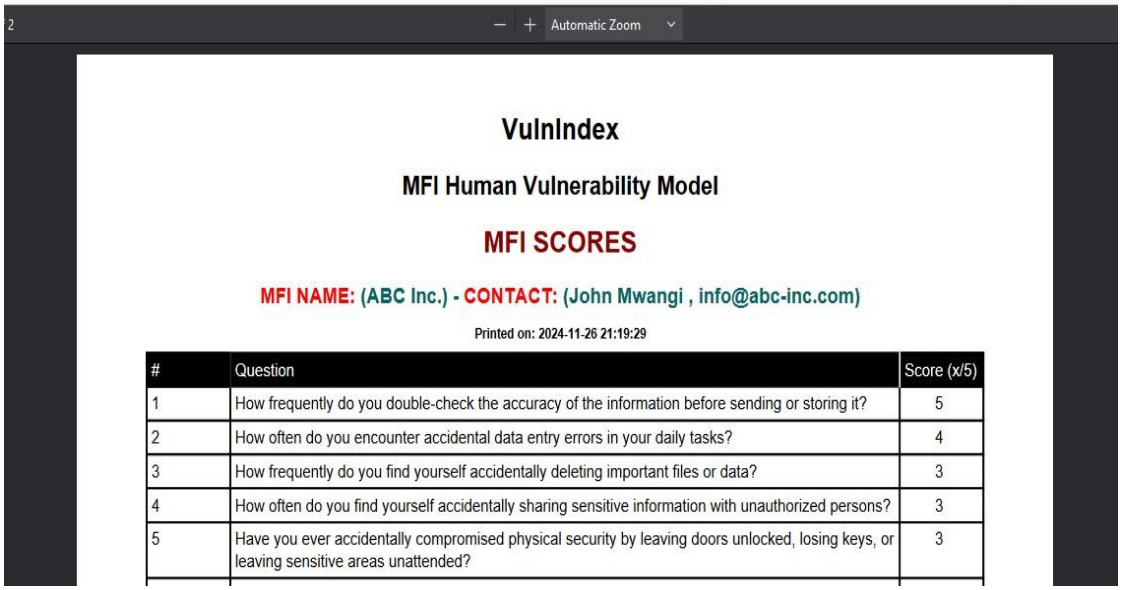


Figure 26: Model Cases

Source: Researcher (2024)

5.5.10 System Reports

Both the MFI user portal and admin portal have the capability of producing varied reports that are useful to the system users and admins. At the MFI user portal, user scores and MFI recommendations reports are produced. 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 recommendations 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. The figures below show the assessment scores report and the recommendations report respectively.



VulnIndex

MFI Human Vulnerability Model

MFI SCORES

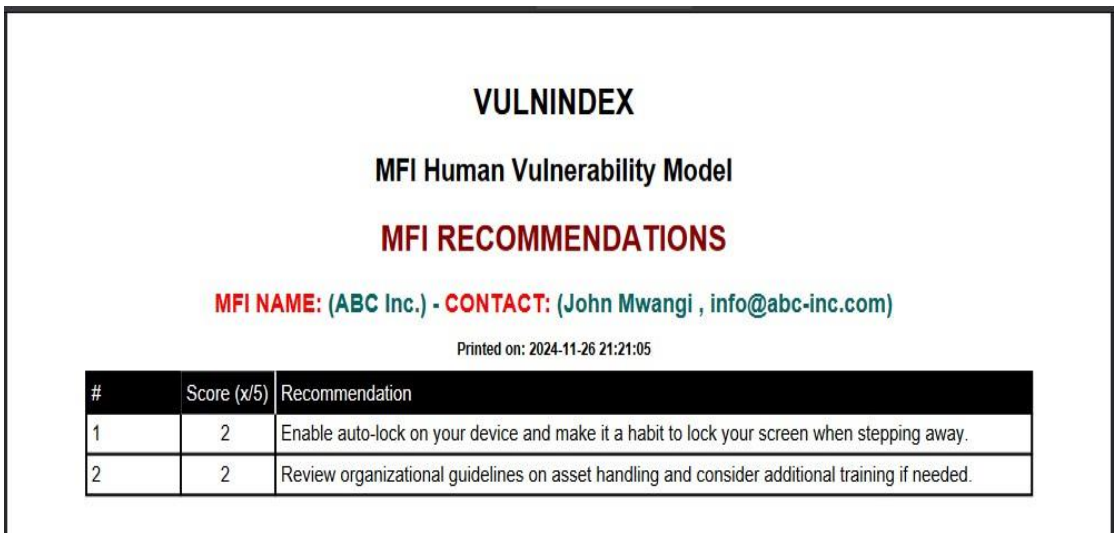
MFI NAME: (ABC Inc.) - CONTACT: (John Mwangi , info@abc-inc.com)

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 5. 9:MFI User Assessment Scores Report

Source: Researcher (2024)



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 5. 10: **MFI Recommendation Report**

Source: Researcher (2024)

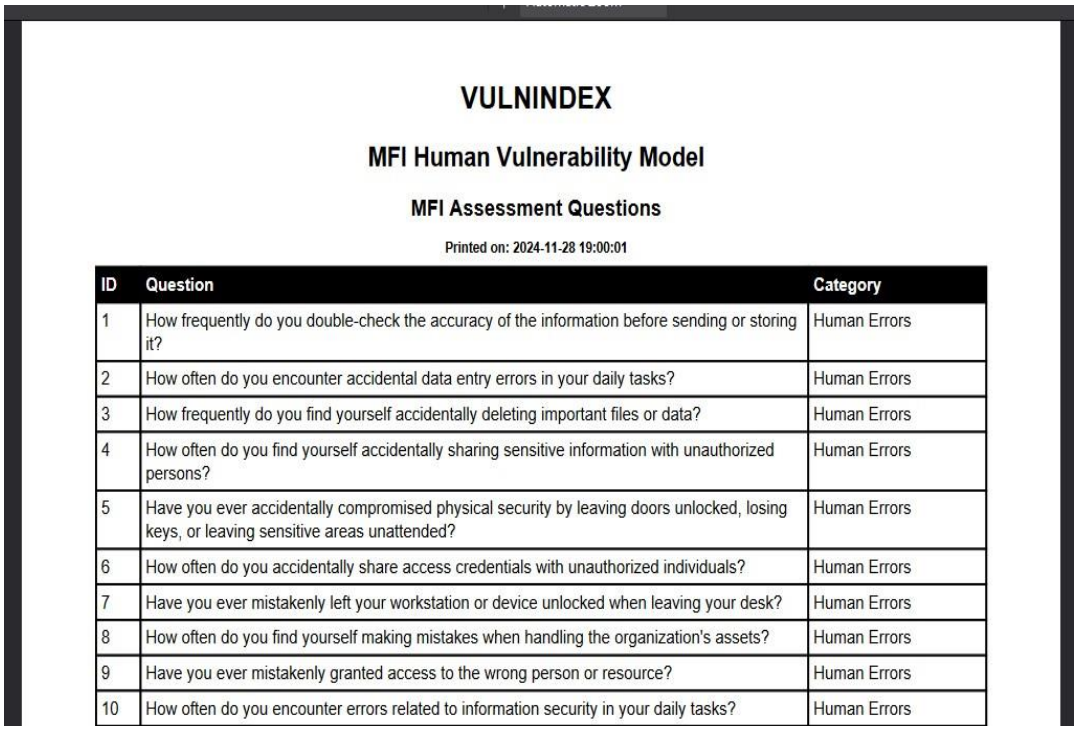
The admin reports include, List of MFIs registered, MFI scores report that indicates the scores that the MFIs achieved when the run assessments, MFI recommendations report, questions report that enable the admin to print the questions usable in the system for assessment. The figures below present admin module reports.

Figure 5. 11 Figure: MFI Assessment Summary

Source: Researcher (2024)

Figure **Figure 5. 12**: **MFI Register List**

Source: Researcher (2024)



VULNINDEX

MFI Human Vulnerability Model

MFI Assessment Questions

Printed on: 2024-11-28 19:00:01

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

Figure 31: MFI Assessment Questions List

Source: Researcher (2024)

5.5.11 MFI User and Admin Help Modules

The MFI users and admins can get guidance on how to use the system appropriately even though friendly UI technologies were used to designed the user and admin modules to make it easy to read and navigate. Help modules guide the user on how to carry out the activities once they login successfully. The user and admin help panels are presented in figures 32 and 33 below.

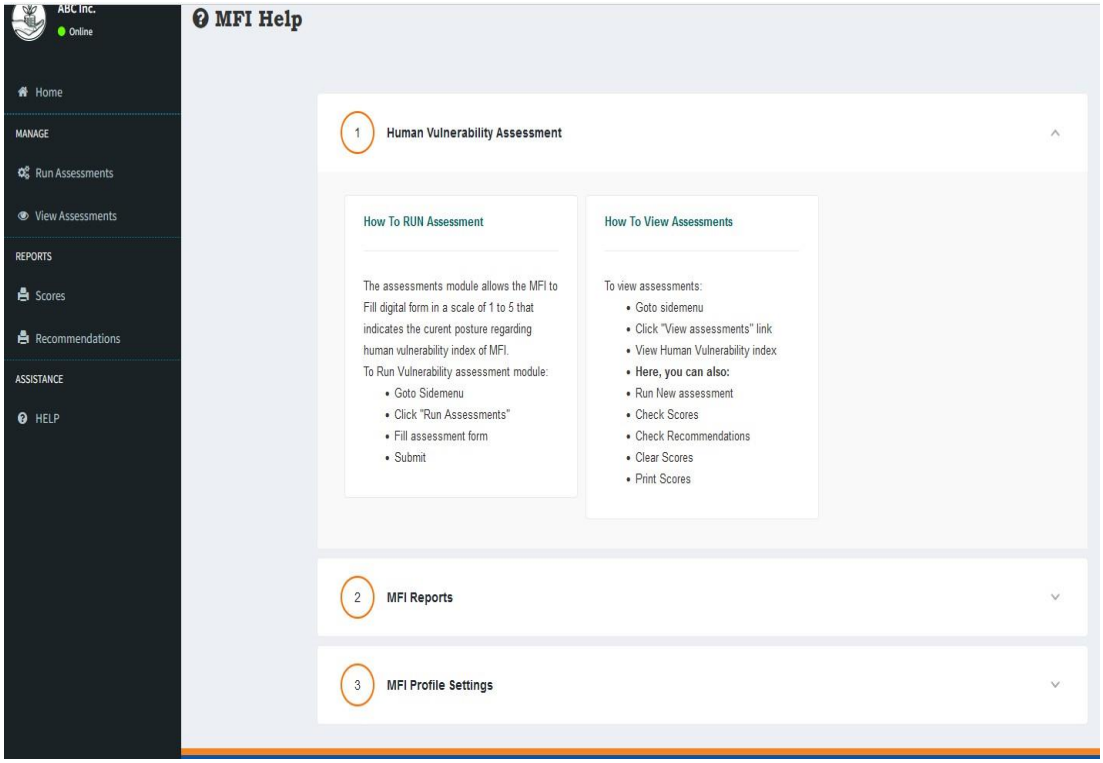


Figure 5. 13 : MFI User Portal Help

Source: Researcher (2024)

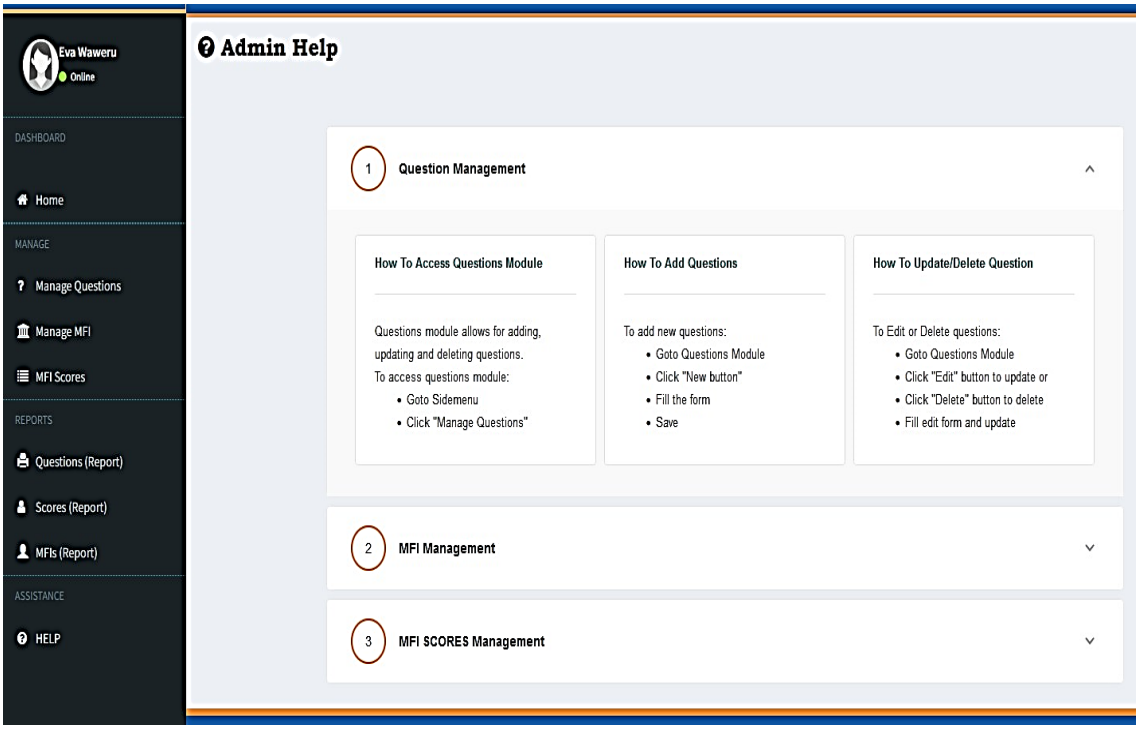


Figure 5. 14: Admin Help

Source: Researcher (2024)

5.5.12 Schema Diagram

The system uses four database tables and one database view to manage users, questions, scores and recommendations. The table names are; Users, Admin, Questions and Assessments. The database view is named assessments_summary_view which generates a summary score for every MFI user when they perform human vulnerability assessment. Figure 34 below presents a summary of the database schema for the model

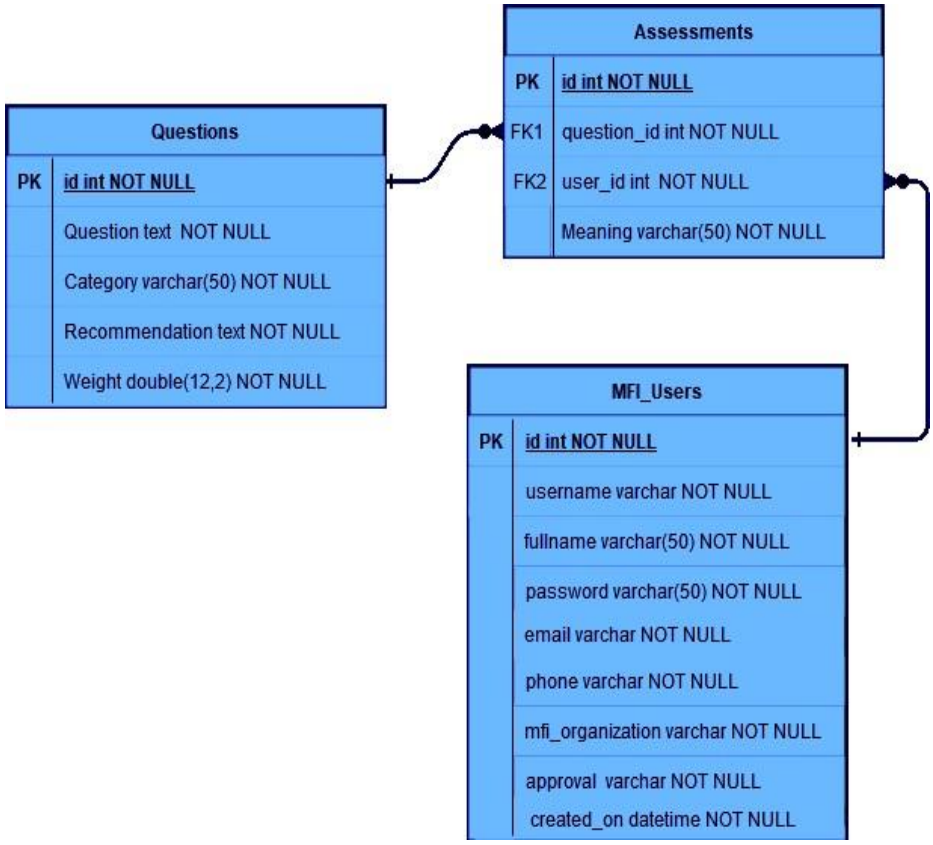


Figure 5. 15: **MFI Vulnerability Schema Diagram**

Source: Researcher (2024)

5.5.13 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.

5.6 Evaluation of the Model

After design, the model was tested to make sure it could fulfill its intended functions. The desired goals were established before the design process began and were used as a checklist of deliverables for evaluation once the design was complete. Together with the desired aims, the achieved outputs are summarized in table 17 below. The table indicates that every goal was accomplished. In conclusion, the system does its intended tasks rather effectively.

Table 5. 1: Objective Evaluation

Components	Goals	Delivered Outcomes
MFI User Registration	Capture MFI user information and post to the Users Database with hashed password.	MFI User Registration Form Accepts MFI User information and posts successfully to MySQL Database. Passwords are successfully Hashed
MFI User Login	Allow users who provide correct user credentials to login and get redirected to User dashboard.	The System Permits Login with Correct credentials and successfully redirects MFI users to user dashboards.
Admin Login	Allow Admins who provide correct admin credentials to login and get redirected to Admin dashboard.	The System Permits Login for admins who provide correct credentials and successfully redirects them to admin dashboards.
Navigation for MFI Users and Admin	Allow easy Navigation within the User portal and Admin portal	Easy navigation using for users and admins facilitated by the side menus on the corresponding portals.

Vulnerability Assessments	Retrieve Questions from database and Present in a Likert scale of 1 to 5 Likert per assessment question then allow posting of MFI user scores to the database	The model retrieves vulnerability assessment questions from database into a Likert scale presented to the user as five radio buttons for each vulnerability assessment question. The scores are successfully posted to the database.
Vulnerability Scores Report	Retrieve assessment scores into a Portable document	The System retrieves Scores for the logged-in MFI users and admin and allow printing of scores to PDF
MFI Recommendations Report	Retrieve Recommendations from the database after assessment into a Portable document	The System retrieves recommendations for the logged-in user and exports it to PDF

5.7 Security of the Model

The three primary principles of information security confidentiality, integrity, and authenticity (CIA) were taken into consideration in the model's construction. The login module's secure authentication and session establishment and removal procedures guaranteed confidentiality. Only those who have registered may log in and access their own records. By guaranteeing that users could only alter their own records and not those of other users, integrity was also maintained. For example, a person may only remove their own prior human vulnerability assessment results—not those of others. In the end, availability was guaranteed by selecting web servers with the lowest downtime records to host the application online. As a result, users may access the system and use its features whenever they choose.

CHAPTER SIX

6. CONCLUSIONS AND RECOMMENDATIONS

6.1 Discussion of Findings and Comparative Analysis

The development and validation of the Cyber Security Human Vulnerability Exposure Index (CSHVEI) model confirm the critical role of quantifiable human factors in the cybersecurity posture of Microfinance Institutions (MFIs). The derived model, CSHVEI = -0.062 + (0.167 × Human Error) + (0.539 × Negligence) + (0.324 × Ignorance), provides a robust tool for assessment, with an Adjusted R^2 of 0.902 indicating that the three consolidated variables explain over 90% of the variance in human vulnerability exposure.

The weighting of the variables offers profound insights. The dominance of Negligence ($\beta = 0.539$) as the primary contributor suggests that within Nairobi's MFIs, deliberate non-compliance and careless behaviour are more detrimental than a lack of knowledge. This aligns with global reports, such as the Verizon DBIR, which consistently highlight privilege misuse and oversight as leading causes of incidents (Grady, 2024). The significant role of Ignorance ($\beta = 0.324$) underscores a critical gap in cybersecurity awareness and training, reinforcing the findings of scholars like Dash & Ansari (2022) on the importance of continuous security education. While Human Error ($\beta = 0.167$) is less weighted, it remains a persistent threat, consistent with Hadlington's (2021) concept of the "accidental insider."

6.1.1 Comparative Analysis with Prior Models

This research was initiated to address specific gaps in existing cybersecurity frameworks concerning the measurement of human factors. A comparative analysis demonstrates the unique contribution of the CSHVEI model: Complementing Broad Frameworks (NIST, ISO 27001): While the NIST Cybersecurity Framework (NIST, 2018) and ISO/IEC 27001 (Lopes et al., 2019) provide essential, high-level guidelines for managing cybersecurity and information security risk, they lack a dedicated, quantitative metric for human factor exposure. The CSHVEI model operationalizes the principles from these standards (e.g., NIST's "Identify" function, ISO's Annex A.7) into a specific, calculable index, providing a tangible outcome from their broader, qualitative guidance.

Addressing the Technical Focus of Existing Tools: Frameworks like the Cyber Visibility and Exposure (CVEQ^TM^) Assessment (Wambalaba et al., 2021) and the OWASP Top Ten (Fredj et al., 2021) are heavily oriented towards technical controls and application vulnerabilities. They often underweight the human element or, in the case of OWASP, do not explicitly cover human-manipulated attacks like social engineering. The CSHVEI model fills

this niche by providing a focused tool that complements these technical assessments, offering a holistic view of both technical and human attack surfaces.

Advancing Human-Focused Models: The Human Factor Vulnerability Analysis (HFVA) model by Ani et al. (2019) is a precedent but is constrained by its reliance on pre-existing technical vulnerabilities. Similarly, the CAT Framework (Hijji & Alam, 2022) focuses on education but lacks a metric to measure its impact on exposure. The CSHVEI model advances upon these by being independent of technical flaws, focusing purely on behavioural outcomes, and providing an empirical index that can, in fact, be used to measure the effectiveness of training initiatives like those proposed by the CAT Framework. The CSHVEI model does not seek to replace these established frameworks but rather to augment them. It plugs a critical gap by providing a specialized, quantitative, and empirically-derived tool specifically designed to measure what other frameworks largely describe qualitatively.

6.2 Limitations of the Study

While this research provides valuable insights, it is subject to several limitations: Scope and Generalizability: The study was confined to MFIs within Nairobi County, Kenya. Although Nairobi is a financial hub, the findings may not be fully generalizable to MFIs in other regions or countries with different regulatory environments and cultural attitudes towards cybersecurity. Furthermore, the model was not tested against other sectors, such as healthcare or large commercial banks, where human factor dynamics might differ.

Sample Size and Subjectivity: The sample size of 112 respondents, while sufficient for the statistical analyses conducted, represents a fraction of the entire MFI sector. The data also relied on self-reported measures through questionnaires, which are susceptible to biases such as social desirability bias, where respondents may answer questions in a manner they believe is favourable rather than being entirely truthful about their security practices.

Implementation Constraints: The web-based prototype served as a proof-of-concept. Its evaluation was primarily functional (alpha and beta testing) and did not include a long-term, longitudinal study to assess its real-world impact on reducing security incidents within MFIs. The security of the model itself, while designed with standard practices, was not subjected to an independent penetration test.Model Simplification: The reduction of nine conceptual variables into three core factors (Human Error, Negligence, Ignorance), while statistically valid and beneficial for model parsimony, may have oversimplified some of the nuanced aspects of human behaviour in cybersecurity.

6.3 Conclusions and Recommendations

6.3.1 Conclusions

This research successfully addressed its objectives by identifying key human factor vulnerabilities, deriving a statistically robust model for the CSHVEI, implementing it via a functional web-based prototype, and validating its utility. The study conclusively demonstrates that human factors are not just an abstract risk but a quantifiable exposure, with negligence being the most significant contributor in the MFI context. The CSHVEI model provides a practical and much-needed tool for organizations to measure, understand, and ultimately mitigate the human element of their cybersecurity risk.

6.3.2 Recommendations

Based on the findings, the following recommendations are proposed:

For MFIs: Adopt the CSHVEI Model: Integrate the CSHVEI assessment into their regular security audits to establish a baseline and track progress over time. Targeted Training Programs: Shift cybersecurity training from generic awareness to targeted interventions focused specifically on combating negligence and promoting a culture of compliance, given its high weighting in the exposure index. Promote a Security-Conscious Culture: Leadership should foster an environment where security is seen as a shared responsibility, and safe practices are recognized and rewarded.

For Policymakers and Regulators: Consider incorporating human factor assessments, guided by frameworks like the CSHVEI, into the cybersecurity compliance requirements for financial institutions, particularly those serving vulnerable populations.

For Future Researchers: Explore the integration of the enhancements listed in section 6.3, particularly the use of AI and behavioural analytics, to create a next-generation human risk management platform.

6.4 Future Enhancements

The CSHVEI model establishes a strong foundation upon which several future enhancements can be built: AI and Machine Learning Integration: Future iterations could incorporate AI algorithms to analyse assessment data over time. Machine learning models could identify subtle patterns and predict potential security breaches based on trending vulnerability scores, moving the model from a diagnostic to a predictive tool. Adaptive Learning and Personalization: The system could be enhanced with an adaptive learning engine. Based on an

MFI's recurring weakness (e.g., consistently high negligence scores), the platform could automatically curate and recommend tailored training modules, videos, and policy templates to address those specific deficiencies.

Inclusion of Behavioural Analytics: Integrating with existing log management or Security Information and Event Management (SIEM) systems could allow for the incorporation of objective behavioural data. For example, metrics on password change frequency, phishing email click-through rates, and access policy violations could be used to complement and validate the subjective survey data, creating a more robust and objective index. Expansion of Scope and Benchmarking: Future research should aim to apply and validate the CSHVEI model in other sectors and geographical locations. Building a large, anonymized dataset would allow for the creation of industry-wide benchmarks, enabling organizations to compare their posture against peers.

REFERENCES

Abebe, G. (2020). *Human Factors Influence in Information Systems Security: Towards a Conceptual Framework.*

Abawajy, J., & Kim, T. H. (2010). Performance analysis of cyber security awareness delivery methods. In *Security Technology, Disaster Recovery and Business Continuity: International Conferences, SecTech and DRBC 2010, Held as Part of the Future Generation Information*

Technology Conference, FGIT 2010, Jeju Island, Korea, December 13-15, 2010. Proceedings (pp. 142-148). Berlin, Heidelberg: Springer Berlin Heidelberg.

Ahola, M. (2019). The role of human error in successful cyber security breaches. *Recuperado de: https://blog. getusecure. com/post/the-role-of-human-error-in-successful-cyber-securitybreaches. Último acceso el*, *5*, 1-11.

Alejandro, L. (2022). *Human Factor in Cybersecurity: The Weakest Link?* Human Factor in Cybersecurity. https://www.kuppingercole.com/events/csls2022/blog/human-factorin-cybersecurity-the-weakest-link

Alghamdi, M. I. (2021). *Effects of Knowledge of Cyber Security on Prevention of Attacks*.

Al-Daeef, M. M., Basir, N., & Saudi, M. M. (2017, July). Security awareness training: A review. In *Proceedings of the world congress on engineering* (Vol. 1, pp. 5-7).

Alkatheiri, M. S., Chauhdary, S. H., & Alqarni, M. A. (2021). Seamless security apprise method for improving the reliability of sustainable energy-based smart home applications. *Sustainable Energy Technologies and Assessments*, *45*, 101219. https://doi.org/10.1016/j.seta.2021.101219

Alkhalil, A., Kadaoure, I., & Kouadio, M. (2020). An Evaluation of 20-m ESA-CCI S2 Prototype LC Product. *Frontiers in Sustainable Food Systems*, *4*. https://www.frontiersin.org/articles/10.3389/fsufs.2020.504334

Alsharif, M., Mishra, S., & Alshehri, M. (2021). Impact of Human Vulnerabilities on Cybersecurity. *Computer Systems Science and Engineering*, *40*. https://doi.org/10.32604/csse.2022.019938

Amr Tolba, et. al. (2021). *Methods of Security Authentication and Authorization into Informationals Systems | IEEE Conference Publication | IEEE Xplore*. https://ieeexplore.ieee.org/abstract/document/9349333

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*,

21(1), 2–35. https://doi.org/10.1108/JSIT-02-2018-0028

Atlam, W. (2020). *IoT Security, Privacy, Safety and Ethics | SpringerLink*. https://link.springer.com/chapter/10.1007/978-3-030-18732-3_8

Bandari, V. (2023). *Bandari, V. (2023). Enterprise Data Security Measures: A Comparative Review of Effectiveness and Risks Across Different Industries and Organization Types. International Journal of Business Intelligence and Big Data Analytics, 6(1), 1-11*.

Calic, D., Pattinson, M. R., Parsons, K., Butavicius, M. A., & McCormac, A. (2016). Naïve and Accidental Behaviours that Compromise Information Security: What the Experts Think. In *HAISA* (pp. 12-21).

Das, A., & Pathak, P. (2022). Risk assessment and mitigation techniques of cyber attacks in emerging technologies. *AIP Conference Proceedings*, *2519*(1), 030042. https://doi.org/10.1063/5.0109616

Dash, B., & Ansari, M. F. (2022). *An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy*. *9*, 2395–0056.

Dawadi, et. al. (2021). *Mixed-Methods Research: A Discussion on its Types, Challenges, and Criticisms—Open Research Online*. https://oro.open.ac.uk/75449/

Dutta, A. (2023). Navigating the Budding Researchers through Different Study Designs in Homeopathy: Part 1 of Research Method Series. *Homœopathic Links*, *36*(2), 128–136. https://doi.org/10.1055/s-0043-57041

Dwivedi, R., Nerur, S., & Mangalaraj, G. (2023). Predicting Insider Breaches Using Employee Reviews. *Journal of Computer Information Systems*, *0*(0), 1–15. https://doi.org/10.1080/08874417.2023.2226640

Fredj, O. B., Cheikhrouhou, O., Krichen, M., Hamam, H., & Derhab, A. (2021). An OWASP Top Ten Driven Survey on Web Application Protection Methods. In J. Garcia-Alfaro, J. Leneutre, N. Cuppens, & R. Yaich (Eds.), *Risks and Security of Internet and Systems* (pp. 235–252). Springer International Publishing. https://doi.org/10.1007/978-3-03068887-5_14

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Detecting Insider Threat via a CyberSecurity Culture Framework. *Journal of Computer Information Systems*, *62*(4), 706–716. https://doi.org/10.1080/08874417.2021.1903367

Ghoreishi, M., & Happonen, A. (2020). New promises AI brings into circular economy accelerated product design: A review on supporting literature. *E3S Web of Conferences*, *158*, 06002. https://doi.org/10.1051/e3sconf/202015806002

Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. *Journal of Cybersecurity*, *6*(1), tyaa005. https://doi.org/10.1093/cybsec/tyaa005

Grady . A. (2024). *The Human Factor in Computer Security: Educating Users to Prevent Vulnerabilities*. Retrieved on 17th November, 2024 from: https://moldstud.com/articles/p- thehttps://moldstud.com/articles/p-the-human-factor-in-computer-security-educating-users-to-prevent-vulnerabilitieshuman-factor-in-computer-security-educating-users-to-prevent-vulnerabilities

Graham, J., Hieb, J., & Naber, J. (2016). Improving cybersecurity for Industrial Control Systems. *2016 IEEE 25th International Symposium on Industrial Electronics (ISIE)*, 618–623. https://doi.org/10.1109/ISIE.2016.7744960

Grassegger, T., & 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

Greitzer, F. L. (2019). Insider Threats: It's the HUMAN, Stupid! *Proceedings of the Northwest Cybersecurity Symposium*, 1–8. https://doi.org/10.1145/3332448.3332458

Greitzer, F. L., Purl, J., Leong, Y. M., & Sticha, P. J. (2019). Positioning Your Organization to Respond to Insider Threats. *IEEE Engineering Management Review*, *47*(2), 75–83. IEEE Engineering Management Review. https://doi.org/10.1109/EMR.2019.2914612

Hadlington, L. (2021). The "Human Factor" in Cybersecurity: Exploring the Accidental Insider. In *Research Anthology on Artificial Intelligence Applications in Security* (pp. 1960–1977). IGI Global. https://doi.org/10.4018/978-1-7998-7705-9.ch087

Hijji, M., & Alam, G. (2022). Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. *Sensors (Basel, Switzerland)*, *22*(22), 8663. https://doi.org/10.3390/s22228663

Hoffmann, J. P., & Shafer, K. (2010). Linear regression analysis: Applications and assumptions. *Brigham Young University, Provo*, 1-285.

ITU Telecom World. (2021, December 17). *Securing cyberspace and protecting privacy: Meeting the challenges of a digital world - ITU Telecom World*. https://digitalworld.itu.int/securing-cyberspace-and-protecting-privacy-meeting-the-challenges-ofa-digital-world/

Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019). Towards an Improved Understanding of Human Factors in Cybersecurity. *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*, 338–345. https://doi.org/10.1109/CIC48465.2019.00047

Joinson, A., & van Steen, T. (2018). Human aspects of cyber security: behaviour or culture change?. *Cyber Security: A Peer-Reviewed Journal*, *1*(4), 351-360.

Jung, Y., Sunyoung, H., Hwang, N., & Jung, S. M. (2021). A Development of a Disaster Ethics Education Program for Nurses Using Rapid Prototyping Model. 군진간호연구, *39*(1), 70–90. https://doi.org/10.31148/kjmnr.2021.39.1.70

Kessler, S. R., Pindek, S., Kleinman, G., Andel, S. A., & Spector, P. E. (2020). Information security climate and the assessment of information security risk among healthcare employees. *Health informatics journal*, *26*(1), 461-473.

Khatri, K. K. (2020). Research Paradigm: A Philosophy of Educational Research. *International Journal of English Literature and Social Sciences*.

Kim, J., & Sohn, M. (2022). Graph Representation Learning-Based Early Depression Detection Framework in Smart Home Environments. *Sensors*, *22*(4), Article 4. https://doi.org/10.3390/s22041545

Kim, J. H. (2019). Multicollinearity and misleading statistical results. *Korean journal of anesthesiology*, *72*(6), 558-569.

Koza, E. (2022). *Semantic Analysis of ISO/IEC 27000 Standard Series and NIST Cybersecurity Framework to Outline Differences and Consistencies in the Context of Operational and Strategic Information Security*.

Krishnasamy, V., & Venkatachalam, S. (2023). An efficient data flow material model based cloud authentication data security and reduce a cloud storage cost using Index-level Boundary Pattern Convergent Encryption algorithm. *Materials Today: Proceedings*, *81*, 931–936. https://doi.org/10.1016/j.matpr.2021.04.303

Kure, H. I., Islam, S., Ghazanfar, M., Raza, A., & Pasha, M. (2022). Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system. *Neural Computing and Applications*, *34*(1), 493–514. https://doi.org/10.1007/s00521021-06400-0

Kumar, U.V & Reddy, E.M. (2023). Preventing Unauthorized Users from Accessing Cloud Data (May 15, 2023). Available at SSRN: https://ssrn.com/abstract=4448543 or http://dx.doi.org/10.2139/ssrn.4448543

Lauff, C., Menold, J., & Wood, K. L. (2019). Prototyping Canvas: Design Tool for Planning Purposeful Prototypes. *Proceedings of the Design Society: International Conference on Engineering Design*, *1*(1), 1563–1572. https://doi.org/10.1017/dsi.2019.162

Lee, I. (2022). Analysis of Insider Threats in the Healthcare Industry: A Text Mining Approach. *Information*, *13*(9), Article 9. https://doi.org/10.3390/info13090404

Li, J. (2020). Vulnerabilities Mapping based on OWASP-SANS: A Survey for Static Application Security Testing (SAST). *Annals of Emerging Technologies in Computing*, *4*(3), 1–8. https://doi.org/10.33166/AETiC.2020.03.001

Lopes, I., Guarda, T., & Oliveira, P. (2019). Implementation of ISO 27001 Standards as GDPR Compliance Facilitator. *Journal of Information Systems Engineering & Management*, *4*. https://doi.org/10.29333/jisem/5888

Malaivongs, S., Kiattisin, S., & Chatjuthamard, P. (2022). Cyber Trust Index: A Framework for Rating and Improving Cybersecurity Performance. *Applied Sciences*, *12*(21), Article 21. https://doi.org/10.3390/app122111174

Mazzarolo, G., & Jurcut, A. D. (2019). *Insider threats in Cyber Security: The enemy within the gates* (No. arXiv:1911.09575). arXiv. https://doi.org/10.48550/arXiv.1911.09575

Mweshi, G. K., & Sakyi, K. (2020). Application of sampling methods for the research design. *Archives of Business Research*, *8*(11), 180–193. https://doi.org/10.14738/abr.811.9042 Miller, B., Miller, K., Zhang, X., & Terwilliger, M. G. (2020). Prevention of Phishing Attacks: A Three-Pillared Approach. *Issues in Information Systems*, *21*(2).

NamLabs Technologies. (2021, June 15). *Application Security: Definition, Types, Tools, Approaches*. DevOps and Software Engineering Glossary Terms | Atatus. https://www.atatus.com/glossary/application-security/

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., &

Bonacina, S. (2021). Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. *Sensors*, *21*(15), Article 15. https://doi.org/10.3390/s21155119

Ogbanufe, O. (2021). Enhancing End-User Roles in Information Security: Exploring the Setting, Situation, and Identity. *Computers & Security*, *108*, 102340. https://doi.org/10.1016/j.cose.2021.102340

Paz, S. (2023). Cybersecurity Standards and Frameworks. In *IEEE Technology and Engineering Management Society Body of Knowledge (TEMSBOK)* (pp. 397–416). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119987635.ch23

Plappert, C., Zelle, D., Gadacz, H., Rieke, R., Scheuermann, D., & Krauß, C. (2021). Attack Surface Assessment for Cybersecurity Engineering in the Automotive Domain. *2021 29th Euromicro International Conference on Parallel, Distributed and Network-Based*

Processing (PDP), 266–275. https://doi.org/10.1109/PDP52278.2021.00050

Platview technologies. (2023). *The Importance of End User Security – Platview*. https://platview.com/the-importance-of-end-user-security/

Pramanik, S., Samanta, D., Vinay, M., & Guha, A. (2022). *Cyber Security and Network Security*. John Wiley & Sons.

Preethiga Narasimman. (2023). *Cyber Security Laws and Regulations of 2023*. https://www.knowledgehut.com/blog/security/cyber-security-laws

Rao, U.H., Nayak, U. (2014). Data Backups and Cloud Computing. In: The InfoSec Handbook. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4302-6383-8_13

S. Shyam Sundar. (2019). *Machine Heuristic | Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. https://dl.acm.org/doi/abs/10.1145/3290605.3300768

Samtani, S., Abate, M., Benjamin, V., & Li, W. (2020). Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 135–154). Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_8

Sangster, M. (2020). When it comes to cyber security, ignorance isn't bliss–it's negligence. *Network Security*, *2020*(12), 8-12.

Sataloff, R. T., & Vontela, S. (2021). Response rates in survey research. *Journal of Voice*, *35*(5), 683-684.

Sav, U., & Magar, G. (2021). Insider Threat Detection Based on Anomalous Behavior of User for Cybersecurity. In D. S. Jat, S. Shukla, A. Unal, & D. K. Mishra (Eds.), *Data Science and Security* (pp. 17–28). Springer. https://doi.org/10.1007/978-981-15-5309-7_3

Septiani, N., Lutfiani, N., Putri Oganda, F., Salam, R., & Tashya Devana, V. (2022). Blockchain Technology in the Public Sector by Leveraging the Triumvirate of Security. *2022 International Conference on Science and Technology (ICOSTECH)*, 1–5. https://doi.org/10.1109/ICOSTECH54296.2022.9829101

Shouran, Z., Priyambodo, T., & Ashari, A. (2019). Information System Security: Human Aspects. *International journal of scientific & technology research*, *8*(03), 111-115.

Sicard, K. (2019). The Need for Disaster Recovery and Incident Response: Understanding Disaster Recovery for Natural Disasters Versus Cyber-Attacks. *The Kennesaw Journal of Undergraduate Research*, *6*(2). https://digitalcommons.kennesaw.edu/kjur/vol6/iss2/4

Solove, D. J., & Hartzog, W. (2022). *Breached!: Why Data Security Law Fails and how to Improve it*. Oxford University Press.

Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information & Computer Security*, *25*(5), 494-534.

Sutton, A., Clowes, M., Preston, L., & Booth, A. (2019). Meeting the review family: Exploring review types and associated information retrieval requirements. *Health Information & Libraries Journal*, *36*(3), 202–222. https://doi.org/10.1111/hir.12276

swarnavo. (2022, February 18). Elements of Cybersecurity. *GeeksforGeeks*. https://www.geeksforgeeks.org/elements-of-cybersecurity/

Taber, K. S. (2018). The use of Cronbach's alpha when developing and reporting research instruments in science education. *Research in science education*, *48*, 1273-1296.

Team, C. (2021, August 18). *What is The CIA TRIAD & its Importance for Cybersecurity*. Website Security Store. https://websitesecuritystore.com/blog/what-is-the-cia-triad/

Tissir, N., El Kafhali, S., & Aboutabit, N. (2021). Cybersecurity management in cloud computing: Semantic literature review and conceptual framework proposal. *Journal of*

Reliable Intelligent Environments, *7*(2), 69–84. https://doi.org/10.1007/s40860-02000115-0

Tolba, A., & Al-Makhadmeh, Z. (2021). A cybersecurity user authentication approach for securing smart grid communications. *Sustainable Energy Technologies and Assessments*, *46*, 101284. https://doi.org/10.1016/j.seta.2021.101284

Triplett, W. J. (2022). Addressing Human Factors in Cybersecurity Leadership. *Journal of Cybersecurity and Privacy*, *2*(3), Article 3. https://doi.org/10.3390/jcp2030029 Tufail, S., Parvez, I., Batool, S., & Sarwat, A. (2021). A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid. *Energies*, *14*(18), Article 18. https://doi.org/10.3390/en14185894

Uddin, M. R., Akter, S., & Lee, W. J. T. (2024). Developing a data breach protection capability framework in retailing. *International Journal of Production Economics*, *271*, 109202.

Walsh, C., & Best, P. (2019). Practitioners' experiences of using blended models within family support: A proof of concept study involving Cognitive-Behavioural Therapy (CBT),

Multisystemic Therapy (MST) and Incredible Years (IY) interventions. *Journal of Family Social Work*, *22*(4–5), 369–388. https://doi.org/10.1080/10522158.2019.1616240

Wambalaba, F., Musuva, P., Ouma, M. J., & Nicos, K. (2021). *Cyber Security Risk Minimization Best Practices-African Experiences*.

Wang, Z., Zhu, H., & Sun, L. (2021). Social Engineering in Cybersecurity: Effect Mechanisms,

Human Vulnerabilities and Attack Methods. *IEEE Access*, *9*, 11895–11910. IEEE Access. https://doi.org/10.1109/ACCESS.2021.3051633

Wani, T. A., Mendoza, A., & Gray, K. (2020). Hospital Bring-Your-Own-Device Security Challenges and Solutions: Systematic Review of Gray Literature. *JMIR mHealth and uHealth*, *8*(6), e18175. https://doi.org/10.2196/18175

Wani, T. A., Mendoza, A., Gray, K., & Smolenaers, F. (2022). Status of bring-your-own-device (BYOD) security practices in Australian hospitals – A national survey. *Health Policy and Technology*, *11*(3), 100627. https://doi.org/10.1016/j.hlpt.2022.100627

Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security*. Cengage Learning.

Woody, C., & Wallen, C. (2022). *Acquisition Security Framework (ASF): Integration of Supply Chain Risk Management Across the DevSecOps Lifecycle*.

Wu, A. Y., Hanus, B., Xue, B., & Mahto, R. V. (2023). Information security ignorance: An exploration of the concept and its antecedents. *Information & Management*, *60*(2), 103753.

Yin, L., Mo, F., Wu, Q., & Long, Y. (2022). Research on Application of Data Encryption in Computer Network Security. In Q. Liu, X. Liu, B. Chen, Y. Zhang, & J. Peng (Eds.), *Proceedings of the 11th International Conference on Computer Engineering and Networks* (pp. 697–704). Springer Nature. https://doi.org/10.1007/978-981-16-65547_75

Zhang, J. (2021). Distributed network security framework of energy internet based on internet of things. *Sustainable Energy Technologies and Assessments*, *44*, 101051. https://doi.org/10.1016/j.seta.2021.101051

Zhang, J., Wang, Y., Yuan, Z., & Jin, Q. (2020). Personalized real-time movie recommendation system: Practical prototype and evaluation. *Tsinghua Science and Technology*, *25*(2), 180–191. Tsinghua Science and Technology. https://doi.org/10.26599/TST.2018.9010118

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-assolution" cybersecurity mindset. *International Journal of Human-Computer Studies*, *131*, 169–187. https://doi.org/10.1016/j.ijhcs.2019.05.005

APPENDICES

A. QUESTIONNAIRE

I am a Master of Science (Cyber Security) student at The Cooperative University of Kenya researching "**A MODEL TO DETERMINE CYBER SECURITY HUMAN VULNERABILITY EXPOSURE INDEX FOR ORGANISATIONS**". This is to humbly request you to answer the questions outlined here below as honestly as you can. Please be aware that the data you submit will only be utilized for this scholarly study and that it will be kept completely anonymous per strict ethical guidelines.

PART A: GENERAL QUESTIONS

SECTION A

BIO DATA

Please tick the most appropriate answer in this section

1. What is your Gender

Male [ ]

Female [ ]

2. What position do you currently hold at your current working station?

Management [ ]

IT Department [ ]

Customer Service [ ]

Operations [ ]

Other (Specify)----------

SECTION B

3. In a scale of 1 to 5, to what extend do you think the following 3 HUMAN VULNERABILITIES are critical to your MFIs**?**

(KEYS: 1=Not Very Critical, 2=Not Critical, 3=Neutral, 4=Critical, 5=Very Critical)

NO.	Questions	1	2	3	4	5
1	Human Errors					
2	Negligence					
3	Ignorance					

SECTION C

4. In the scale of 1 to 5, please tick the most appropriate answer to the questions here below in relation to HUMAN ERRORS

HUMAN ERRORS

(KEYS: 1= Never, 2 = Rarely, 3= Sometimes, 4= Often, 5 =Always)

NO.	Questions	1	2	3	4	5
1	How frequently do you double-check the accuracy of the information before sending or storing it?					
2	How often do you encounter accidental data entry errors in your daily tasks?					
3	How frequently do you find yourself accidentally deleting important files or data?					
4	How often do you find yourself accidentally sharing sensitive information (e.g., via email, or messaging platforms) with unauthorized persons?					
5	Have you ever accidentally compromised physical security by leaving doors unlocked, losing keys, or leaving sensitive areas unattended?					
6	How often do you accidentally share access credentials with unauthorized individuals (e.g., through email, messaging apps)?					
7	Have you ever mistakenly left your workstation or device unlocked when leaving your desk)?					
8	How often do you find yourself making mistakes when handling the organization's assets?					
9	Have you ever mistakenly granted access to the wrong person or resource?					
10	**How often do you encounter errors related to information security in your daily tasks?**					
11	Have you ever shared confidential information with unauthorized individuals?					

12	Have you ever mistakenly deleted or modified important data that affected the recovery process?					

SECTION D

5. In the scale of 1 to 5, please tick the most appropriate answer to the questions here below in relation to NEGLIGENCE

NEGLIGENCE

(*KEYS: 1= Never, 2 = Rarely, 3= Sometimes, 4= Often, 5 =Always)*

NO.	Questions	1	2	3	4	5
1	How often do you bypass or ignore security protocols (e.g., using weak passwords, sharing login credentials) to save time or for convenience?					
2	How often do you leave your workstation unlocked or your computer unattended while logged into the system?					
3	How often do you leave your computer unattended without locking it?					
4	How regularly do you update your passwords as per the organization's policy?					
5	How often do you notice colleagues disregarding physical security protocols (e.g., tailgating, propping open doors)?					
6	**Are Background Checks conducted** on potential employees to assess their reliability and trustworthiness before hiring?					
7	Have you ever shared your work-related passwords with colleagues?					
8	Have you received training on how to manage access control (e.g., creating strong passwords, securing devices)?					
9	How frequently do you observe negligence or careless behaviour related to asset management among your colleagues?					

10	Do you consistently update your passwords or follow secure password practices.**?**					
11	I leave my workstation without logging out of systems or devices..					
12	I do not regularly verify that my data backups are functioning properly.					

SECTION D

6. In the scale of 1 to 5, please tick the most appropriate answer to the questions here below in relation to IGNORANCE

IGNORANCE

(*KEYS: 1= Never, 2 = Rarely, 3= Sometimes, 4= Often, 5 =Always)*

NO.	Questions	1	2	3	4	5
1	Does your organization offer sensitization programs on information security policies awareness?					
2	Do you know the proper procedures for reporting a security incident in your organization					
3	Do you receive formal training on information security after every 12 months?					
4	Do you know the proper procedures for reporting a security incident in your organization?					
5	Are you aware of the procedures to follow in case of a physical security breach (e.g., unauthorized access, break-in)?					
6	How often do you refer to the organization's guidelines when performing tasks?					
7	Do you know how to identify potential risks or mistakes in your work before they become significant issues?					
8	Do you regularly update your passwords and follow the organization's guidelines for strong password creation?					

9	How often do you ignore or delay following up on security alerts or recommendations related to access control?					
10	How often do you or your colleagues seek guidance when unsure about asset management procedures?					
11	I prioritize my work over following strict security protocols.					
12	I am confident I can handle a security incident without needing formal recovery planning.					

B. INFORMED CONSENT PROCEDURE

THE CO-OPERATIVE UNIVERSITY OF KENYA

INFORMED CONSENT TO PARTICIPATE IN A RESEARCH STUDY

This Informed Consent Form is for study participants whom we are inviting to participate in research entitled **'A model to determine Cybersecurity human factor exposure index for Organizations'**

Evaline Waweru
ewaweru@cuk.ac.ke
0713683472

Prof. Simon Karume
skarume@kabarak.ac.ke
0722499397

Alex Kibet
alexkibet@kabarak.ac.ke
0717470102

You will be given a copy of the full Informed Consent Form

This Informed Consent Form Has Two Parts:

1. Information Sheet (to share information about the research with you)
2. Certificate of Consent (for signatures if you agree to take part)

PART I: INFORMATION SHEET

Introduction

I am Evaline Waweru, a Masters student at Cooperative University. We are researching **"A model to determine Cybersecurity human factor exposure index for organizations".** This research aims to enhance our comprehension of the elements that influence human performance and welfare in work-related settings. You were selected as a possible participant in this study

because of your experience in cybersecurity-related issues. Before you decide, you can talk to anyone you feel comfortable with about the research.

Purpose

The purpose of this study is to develop a model that would provide the following deliverables; a report on cyber security human factors vulnerabilities in organizations, a derived cyber security human factor exposure index model, a model to determine cyber security human factor exposure index and a verified and validated model report on determining cyber security human factor exposure index

Procedures:

Your participation will entail the following:

Filling out questionnaires and surveys on your experiences and working environment.

Potential interviews or focus group discussions to gather qualitative data.

Examination of currently available organizational data, such as incident reports and staff performance records, among others.

Risks and Benefits: Strict confidentiality will be put in place to enhance the protection of privacy and identity during the participation of the research study since it can be subjected to risks related to the disclosure of personal information. The merits of this research include the development of a model that can enhance organizational practices, leading to improved working conditions as well as increased overall well-being in the workplace.

Confidentiality: All data collected for this study will be treated with the utmost discretion. Your identity will be kept private, and anonymity will be maintained by reporting data in aggregate form.

Completely Voluntary Participation: There is no requirement to participate in this study. You are free to withdraw from the study at any moment, for any reason, and without facing any repercussions.

Contact Information: If you have any questions, concerns, or complaints about the research study, please contact the following. Evaline Waweru ewaweru@cuk.ac.ke
0713683472

Prof. Simon Karume
skarume@kabarak.ac.ke
0722499397

Alex Kibet alexkibet@kabarak.ac.ke

0717470102

PART II: CERTIFICATE OF CONSENT

I have read the information provided in this consent form. I had the opportunity to ask questions about it, and all my questions were answered satisfactorily I willingly give my consent to be a participant in this study.

Name _____ Signature _____Date _____

Day/month/year

I have witnessed the accurate reading of the consent form to the potential participant, and the individual has had the opportunity to ask questions. I confirm that the individual has given consent freely.

Name _____ Signature _____Date _____

Day/month/year

Statement by the researcher

I have accurately read out the information sheet to the potential participant, and to the best of my ability made sure that the participant understands that the following will be done;

Participation in this research is entirely voluntary

The information to be collected from this research project will be kept confidential

Knowledge gained from the research will be shared during the last meeting before it is made widely available to the public

…. (if any other that may arise)

I certify that the participant was given the chance to ask questions concerning the study and that I have accurately and fully addressed each question to the best of my abilities. I certify that the consent was freely and voluntarily provided by the individual and that they were not forced to give it.

A copy of this ICF has been provided to the participant.

Name _____Signature _____Date _____

Day/month/year

C. INFORMED CONSENT COMPREHENSION CHECKLIST

ENROLLMENT INFORMED CONSENT COMPREHENSION CHECKLIST			
Name or PTID: ……		Date:	…….
INSTRUCTIONS: Ask each question and then check each item that participants understand during the discussion without a detailed explanation of the correct answer. While running the checklist, you can provide additional explanations for the question and validation of the answers, but additional explanations for the correct answer should only be provided after the entire checklist is complete. After completing the checklist, explain/advise for items that participants cannot prove their understanding, but please do not check these items. Instead, use comment columns to document follow-up discussions and results. If you check the item, the comment category an orb will be displayed. For unchecked items, comment category c is normally displayed, but category d may also be displayed.			
Open-Ended Question/Statement	Required Points of Comprehension	✓	Comments

1	Please describe your understanding of the purpose of the study.	a. Developing a model for determining cyber security human factors exposure index for organizations		
		To derive, implement, and validate the model for the cyber-security human factor exposure index		
2	Please tell me why you were selected as a potential participant in this research study	Because of my experience in the organization		
		b. I am good at cybersecurity		
3	What are participants being asked to do? in this study?	a. to identify the cyber security human factor vulnerabilities in the organization?		
4	What is the purpose of this study?	To develop a model to determine cyber security human factor exposure index and a verified and validated model report on determining cyber security human factor exposure index		
5	how is the participation in this study?	a. participation in this research is entirely voluntary		
6	What are the benefits of participating in this study?	a. future merits should be mentioned		

7	what is the research duration?	a. 4 weeks		
8	What should participants do if they have questions or concerns about what is happening in the study?	a. ask questions either directly or reach out to the given contacts		
9	What are the possible benefits for participants in the study?	a. Information about participants is confidential and private		
		b. Only people working on the study have access to her information		
10	how will this research share the knowledge gained?	a. during the final meeting		
		b. confidential information will not be shared		

OUTCOME: Demonstrated comprehension of all required points, and decided to enrol in the study. Demonstrated comprehension of all required points, decided NOT to enrol in the study. Demonstrated comprehension of all required points, and deferred enrolment decision. Did not demonstrate comprehension of all required points (yet), needs more time/discussion. Unable to demonstrate comprehension of all required points, the consent process was discontinued. Other (specify):_____	Optional Comment Codes: Answered correctly on the first try Could not answer at first but answered correctly with probing Answered incorrectly at first but answered correctly after discussion Not able to answer correctly at this time Other (describe)…… ……..
Researcher Signature: ……	

D. GUIDELINES FOR CONDUCTING THE FOCUS GROUP

The statement of purpose

The focus group discussion approach in this research helped in providing researchers with a deeper understanding of participants' perspectives, experiences, and attitudes. It aimed to define the projected model's requirements and to validate the model based on the discussed feature. It aimed to obtain data from a purposely-selected group of individuals with knowledge and experience in cybersecurity-related issues.

Sampling Procedures for Focus Groups

The focus group was taking between 5-7 members per group as guided by Krueger and Casey (2002). The goal of the study was taken into account while deciding who to invite to the group interview. Members of the focus groups were also chosen based on their knowledge. Members with knowledge and experience in cyber security are the ideal candidates. In the focus group, a homogeneous audience is the goal.

Focus group pattern

The pattern for introducing the group discussion includes: 1) Welcome, 2) Overview of the topic, 3) Ground rules, and 4) First question.

FOCUS GROUP INTRODUCTION

Welcome

Thank you so much for agreeing and willing to participate in the focus group discussion. Please feel appreciated!

Introductions

Moderator and assistant moderator…

Purpose of Focus Groups

Our goal is to develop a cyber-security human factor exposure index model. We are holding these focus groups to clarify the requirements for the model. Please feel free to give us your honest, open opinions; we would appreciate hearing from you.

Ground Rules

1. We Want You to Do the Talking. We would like everyone to participate. I may call on you if I have not heard from you in a while.
2. There Are No Right or Wrong Answers Every person's experiences and opinions are important. Speak up whether you agree or disagree. We want to hear a wide range of opinions.

3. What Is Said in This Room Stays Here We want folks to feel comfortable sharing when sensitive issues come up.

4. We Will Be Tape Recording the Group We want to capture everything you have to say. We don't identify anyone by name in our report. You will remain anonymous.

Engagement questions:

1. Have you ever encountered phishing attempts or social engineering attacks at your workplace? If so, how did you handle the situation?
2. What measures do you think can be implemented to enhance the resilience of employees against phishing and social engineering attacks?
3. How do you manage your passwords for different systems and applications at work?
4. What precautions do you take to ensure the security of your devices and sensitive data when working remotely or outside the office?

System requirements:

1. As an admin of a Cyber security human factor model, what would you want?
2. As a model user, what would you want?
3. What type of user experience would you want?
4. How would you design a Cyber security human factor exposure index model?

E. NACOSTI LICENSE

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Ref No: **295280**

Date of Issue: **10/May/2025**

RESEARCH LICENSE

This is to Certify that Miss.. EVALINE NJERI WAWERU of The Cooperative University of Kenya, has been licensed to conduct research as per the provision of the Science, Technology and Innovation Act, 2013 (Rev.2014) in Nairobi on the topic: A MODEL TO DETERMINE CYBER SECURITY HUMAN VULNERABILITIES EXPOSURE INDEX FOR MFIs IN NAIROBI CITY COUNTY, KENYA for the period ending : 10/May/2026.

License No: **NACOSTI/P/25/4172820**

295280

Applicant Identification Number

Deputy Director
NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Verification QR Code

NOTE: This is a computer generated License. To verify the authenticity of this document, Scan the QR Code using QR scanner application.

See overleaf for conditions

F. SIMILARITY AND AI CONTEST TEST REPORTS

Evaline Waweru

Thesis

Thesis_proposal submision

Phd_Msc_Cohort_1

The Cooperative University of Kenya

Document Details

Submission ID
trn:oid:::1:3313998412

Submission Date
Aug 15, 2025, 12:02 PM GMT+3

Download Date
Aug 15, 2025, 12:31 PM GMT+3

File Name
EvalineFinalDocumentthesis.docx

File Size
2.8 MB

135 Pages

34,272 Words

208,025 Characters

turnitin Page 1 of 156 - Cover Page Submission ID trn:oid:::1:3313998412

18% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text

Exclusions

- 1 Excluded Source

Match Groups

322 Not Cited or Quoted 14%
Matches with neither in-text citation nor quotation marks

111 Missing Quotations 4%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

14% Internet sources
13% Publications
0% Submitted works (Student Papers)

Integrity Flags

1 Integrity Flag for Review

Hidden Text
32 suspect characters on 1 page
Text is altered to blend into the white background of the document.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

- 322 Not Cited or Quoted 14%
  Matches with neither in-text citation nor quotation marks
- 111 Missing Quotations 4%
  Matches that are still very similar to source material
- 0 Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- 0 Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

14% Internet sources
13% Publications
0% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet	www.distinguished-mag.com 1%
2	Internet	library.kabarak.ac.ke <1%
3	Internet	ismsalliance.com <1%
4	Internet	pmc.ncbi.nlm.nih.gov <1%
5	Internet	pcs.usp.br <1%
6	Internet	www.coursehero.com <1%
7	Internet	etd.aau.edu.et <1%
8	Publication	Gulsebnem Bishop. "Cybersecurity Culture", CRC Press, 2025 <1%
9	Internet	www.researchgate.net <1%
10	Internet	www.fortinet.com <1%

G. PUBLICATION

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