UNIVERSITY OF LUSAKA

C

SCHOOL OF POSTGRADUATE STUDIES

AN ANALYSIS OF THE EFFECTS OF CYBER THREATS ON THE UPTAKE OF DIGITAL FINANCIAL SERVICES IN KITWE (CHISOKONE) - ZAMBIA

A Dissertation Submitted to the school of postgraduate studies, University of Lusaka in partial fulfillment to the University of Lusaka of the award of the Master of Science in Risk Management

BY

PYTHIAS KAMANGA

MRM212483891

JANUARY 2024

DECLARATION

I Pythias Kamanga do hereby declare that this research is my authentic work and has never been submitted before in any other university. The publications of other scholars, people, websites, and organizations have been recognized as citations and references.

Signature: 

Date: 26th March 2024

The research report has been submitted for examination with my approval as a University Supervisor.

Supervisor: Ms. Sampa. B. Kangwa

Signature: 

Date: 26th March, 2024

DEDICATION

The study is dedicated to my daughters Prosper and Maya and my lovely wife Precious for your unwavering support.

Abstract

This study explores the impact of cyber threats on the adoption and usage of digital financial services in Kitwe (Chisokone), Zambia. Amidst the rapid digital transformation, this research provides a comprehensive understanding of the digital financial landscape, highlighting the availability and accessibility of various digital financial platforms, the nature and frequency of cyber-attacks, the perceived security of these platforms, and the effectiveness of regulatory protections for users. Employing a mixed-method approach, including surveys and literature review, the study gathers data from both users and providers of digital financial services. The findings reveal that while digital financial platforms are widely available and generally user-friendly, there is a significant prevalence of cyber-attacks, such as hacking and phishing, which raises concerns about the security measures in place. Moreover, the study uncovers a notable discrepancy between users' perception and the actual effectiveness of regulatory authorities in monitoring and safeguarding these platforms. The research concludes with the recommendation for enhanced security protocols, improved user education, and strengthened regulatory oversight to bolster the resilience and trustworthiness of digital financial services in Zambia. This study contributes to the understanding of digital finance in a developing economy context, offering insights for policymakers, financial service providers, and users to navigate the challenges posed by cyber threats effectively.

***Keywords*:** Cyber threats, user security, regulatory oversight, and financial technology (FinTech) in Kitwe, Zambi

List of abbreviations

DFS: Digital Financial Services

DFP: Digital Financial Platform

IMF: International Monetary Fund

UNDP: United Nations Development Programme

SDGs: Sustainable Development Goals

FI: Financial Institutions

DoS: Denial of Service

FinTech: Financial Technology

TABLE OF CONTENTS

CHAPTER ONE

INTRODUCTION AND BACKGROUND

1.0 Introduction

Digital finance can be seen as the impact of modern technologies on the financial services industry that has led to new products, services, processes, and ways of doing business in the banking and financial services sector. According to the prior studies by UNDP, digital finance has played a vital role in complimenting various United Nations Sustainable Development Goals (SGDs) such as the gender equality (SDG 5), decent work and economic growth (SDG 8) and reducing inequalities (SDG 10). The impact of digital finance is in areas such as the Sub-Saharan Africa with generally poorly developed traditional banking infrastructure (UDNP, 2018).

Further studies have shown that new innovations in digital financial technologies are creating new ways of connecting people and institutions using internet and mobile networks thereby getting rid of the need for traditional banking infrastructure. This has made it possible for people to have access to financial service remotely with the use of simple devices such as mobile phones (Gapp, Ariel, Bessis, Goble, & Obodoekwe, 2021).

The term digital financial services encompass all electronic installments, including retail installments via card or mobile phones. Specialists are the fundamental to digital financial services as they enable clients to access their records from any providers of digital financial services without the need to get to the traditional physical banking halls. Also, core to digital financial services and phone-based payment system is mobile money service. Mobile money services provide electronic wallets and also facilitate payment for goods and services.

Douglas and Loader define cybercrime as computer enabled activities performed through global electronic networks which are either illegal or considered unsuitable by certain

parties. In order to put in place appropriate cyber security measures, businesses and individuals must have a good understanding of the effects and impacts of cyber threats or cybercrime. Further, providers of digital financial services need to be aware of Internet threats and must consider all those measures that can help in improving the awareness of individual users with regard to safety and safe financial business environment. They contend that cyber threats have effects on the integrity of financial institutions and other organizations. Therefore, for appropriate measurements to be put in place, organizations must have a good understanding of the effects of cyber threats (Douglas & Loader, 2020).

1.1. Background of the Study

A study conducted by Maurer and Nelson (2021) showed that in February 2016, hackers targeted the central bank of Bangladesh and exploited vulnerabilities in SWIFT, the global financial system's main electronic payment messaging system, caused a loss of one billion United States dollars. In as much as most of the attempted transactions were blocked, over one hundred million United States dollars was stolen in the process. This heist was a wake-up call for the leaders in the finance world that systemic cyber risks in the financial system had been severely underestimated. Today, the assessment that a major cyberattack poses a threat to financial stability is self-evident, it is not a question of if, but when. Yet the world's governments and companies continue to struggle to contain the threat because it remains unclear who is responsible for protecting the system. Increasingly concerned, key voices are sounding the alarm. In February 2020, Christine Lagarde, president of the European Central Bank and former head of the International Monetary Fund, warned that a cyberattack could trigger a serious financial crisis. In April 2020, the Financial Stability Board (FSB) warned that "a major cyber incident, if not properly contained, could seriously disrupt financial systems, including critical financial infrastructure, leading to broader financial stability implications." The potential economic costs of such events can be immense and the damage to public trust and confidence significant (Maurer & Nelson, 2021).

According to Silvia ((Silvia, Judith, & David, 2019)., digital financial services help in improving people's lives through enhanced financial inclusion. Unfortunately, the study revealed that cybercrime has become a major source of concern for financial markets in

developing countries. For instance, over the recent past, financial markets in Sub-Saharan Africa, the Asia and Latin America have been affected by a rapid increase in the number of cyber incidents and data breaches and the most affected have been those markets with higher volumes of digital financial services transactions (Silvia, Judith, & David, 2019).

Asian financial markets have the highest usage of mobile banking and digital payment applications, but they are also experiencing the highest volume of cyberattacks on financial institutions. For instance, in 2016, financial institutions in countries such as Bangladesh, Indonesia, Japan, the Philippines, Taiwan and Viet Nam were targeted in a series of attacks. In Sub-Saharan Africa and Latin America, cybercrime is also on the rise, with cyber-criminal communities in these two regions growing faster than anywhere else. One explanation for these trends may be the fact that DFS transactions are often carried out using insecure devices and over transmission lines that were not designed to protect the security of financial transactions, which leaves DFS systems and providers more vulnerable. Furthermore, with developed economies building up their defenses against cyberattacks, cyber criminals seem to be shifting their attention to easier targets in emerging DFS markets and exploiting their vulnerabilities (Silvia, Judith, & David, 2019). The introduction of digital financial services (DFS) offers new opportunities to reduce the transaction costs associated with money transfers. Over the past decade, the number of DFS deployments has increased substantially, with over 300 deployments worldwide as of 2020. While there is substantial potential for such services to address the constraints to financial inclusion, especially in West Africa, widespread adoption and usage of these services remains relatively concentrated in particular markets. Economic research shows promise in terms of DFS increasing access to money transfers, smoothing consumption and reducing poverty in the long-term, but few studies have more sustained impacts (Jenny & David , 2022).

Across sub-Saharan Africa, access to formal financial services has grown rapidly over the past decades, and especially in the common currency zone of West Africa (WAEMU). While precise estimates differ, surveys suggest that 35% of the adult population in WAEMU held an account at a formal financial institution as of 2014, with similar estimates

in 2017. Despite these advances, there is still significant heterogeneity in financial inclusion within and across the region. Niger and Togo offer a helpful contrast while Niger has the lowest take-up of formal financial accounts and mobile money accounts (16%), Togo has the highest at 45%. Beyond heterogeneity across countries, there is also intra-country variation in access to financial services, often driven by socioeconomic and demographic indicators. In general, those with access to formal financial services are more likely to be male, have a secondary education, and higher levels of income.

Digitization has become an easier platform to support financial inclusion and female financial empowerment. Obstacles to financing access, such as physical distance, minimum balance requirements, little to no credit, and low-income flows can be circumvented. Savings have increased, micro-savers have opened bank accounts, and banks are now able to price short-term loans. In fact, currently there are over 20 million virtual savings accounts (one bank accounts for 18 million of these virtual savings accounts five years after the product was launched) that have been opened in the last five years compared to about 30 million deposit accounts in the banking sector. Not only has digitization in Africa brought financial services to the doorstep, but it has also been an important avenue for creating market access. The benefits are clearly widespread and attractive, and new virtual savings products and platforms continue to emerge (Wechsler & Siwakoti, 2018).

According to the survey conducted by Finscope, the financial inclusion rate in Zambia stood at 59% in 2015 (Finscope Zambia, 2015).The Ministry of Finance's 2017 to 2022 financial inclusion strategy for instance states that the inclusion rate in 2015 was only 59% in Zambia with 49.9% of rural dwellers financially excluded and financial services access points were concentrated in Lusaka and Copper belt provinces. Therefore, the rise of Digital Financial Services (DFS) presents an opportunity for providing financial services to both the served and underserved (Kabala & Seshamani, 2016). The 2020 Finscope Zambia report shows that the financial inclusion rate for Zambia increased by over 10% to 69.4% from 59% percent in 2015. This increase was attributed to an increase in the provision of digital financial services mainly by MNOs and Financial institutions (Finscope Zambia, 2020).

In Zambia, the use of Digital Financial Services (DFS) started with the launch of the now defunct Celpay Zambia Limited in Zambia in 2002 (Kaulu, 2018). Zambian based telecommunications leading firms and other start-ups had strategically positioned themselves for entrance into the digital financial space by the end of the global financial crisis in 2008. For instance, Zambia saw the emergence of mobile money services in 2009 (Kaulu, 2018). By 2011, Mobile Network Operators (MNO) in Airtel and MTN had launched their DFS (Kabala & Seshamani, 2016). By June 2017, ZAMTEL, a government owned Mobile Network Operator also announced the introduction of a mobile payment solution for ZAMTEL customers called ZAMTEL Kwacha. Prior to its launch, ZAMTEL Kwacha was only being used by employees internally for disbursements (Kaulu, 2018). Among the banks, Zambia National Commercial Bank (ZANACO) was the first to launch a mobile banking solution through the introduction of Xapit in 2007 (Kaulu, 2018)

According to Mutambo (Mutambo, 2018), he attributed lack or weak cyber laws in Zambia as one of the most critical challenges to fighting cybercrime. He argued that Zambia does not have a comprehensive legal structure not only to deter but also to prosecute cybercrime. He stated that Zambia only depended on the international and national approaches to cybercrime, with a hope of providing guidance for an effective framework capable of addressing this new crime. He further argued that despite the existence of the Computer Crimes and Misuse Act no.13 0f 2004 which now criminalizes some cybercrimes does not prohibit other major cybercrimes. He also argued that in its current form, the Computers Crimes Act no. 13 of 2004 imposed lighter sentences for offences that require hefty punishments. Finally, in his study he expressed concerns that the statistics of cybercrime in the country do not reflect the actual level of cybercrimes due to the fact that most cybercrime related cases were not being reported by the victims (Mutambo, 2018).

According to (Kaulu, 2018) Digital Financial Services (DFS) have increasingly become a part of the way of doing business not only in Zambia but worldwide. However, he was quick to mention that digital finance was still in its infancy stage in Zambia as many digital financial services were yet to be introduced. This, therefore, presents many opportunities for further development of the digital finance in Zambia's marketplace. He however, noted

that there is need for Zambia to invest in the necessary technology as most of the technology infrastructure currently being used was outdated. He noted that the situation is unlikely to change unless there is massive investment in new technology infrastructure. He further stressed the need for regulators to keep an eye on what is happening in countries where the said technology has been approved so that the country is ready to manage the consequences of this technology when stakeholders decide to introduce it (Kaulu, 2018).

1.1.1 Cyber Threats in Zambia

Zambia has in the recent past seen growth in the usage of digital financial platforms. For instance, the government has introduced Zamportal, a platform that enables the public access different government services. Zamportal is a one-stop shop for all government services. Through this platform, members of the public are able to pay for services electronically without needing to visit a government building facility to make payments. For instance, licenses for registration of companies with PACRA, road tax with RTSA etc. can be paid digitally using this platform. Further, Zambia has seen the mushrooming of mobile money services. Mobile money operators provide users upon registration electronic wallets, which enables the users to receive, stall and send money. The emergence of the mobile money services has pushed banks to also innovate by introducing other digital financial services such as mobile and internet banking. Further, banks and other financial institutions have innovated further by introducing digital ways of providing financial services to their clients. For instance, banks and other microfinance institutions allow clients to access loans online. Insurances companies also allow their clients to purchase insurance policies online. However, these innovations expose users to cyber threats such as internet scams and fraud. For instance, fraudsters engage in criminal activities such as sending links to people when one clicks on the link it directs them to other link and the fraudsters can steal confidential information. The most common cyber threat in Zambia is where fraudsters send random messages to users of mobile money services requesting them to send money or to perform certain transactions. This has in certain instances led to users losing money to fraudsters. It is evident that digital innovation has also come with an increase to digital threats both to users and providers.

In Zambia, providers have taken the initiative to sensitize users against cybercrime through sending users messages and also sensitization campaigns on radio and TV stations. Therefore, this study seeks to analyze the effects that cyber threats may have on the uptake of digital financial services in Zambia.

The following common issues make African cyberspace an attractive target for motivated threat actors:

i. Human factor: While a problem worldwide, Zambia suffers from a general lack of public cyber threat awareness and digital hygiene. Researchers have cited difficulties in disseminating security materials, influenced by factors such as high illiteracy levels. Therefore, there is need to intensify digital education both by Regulators and providers of DFS (Joanna, Januray 2020).
ii. Lack of capacity: Research in 2019 showed only 4 percent of information assurance specialists were located in Africa. By 2020 there was also an estimated shortage of 100,000 cybersecurity professionals on the continent, further hampering organizations' ability to implement proper cybersecurity protocols and tooling (Nir, 2019).
iii. Resources: The majority of countries in the developing world (including Zambia) rely on outdated, poorly secured, unlicensed, or unmanaged information security assets (Joanna, Januray 2020). Numerous countries in Africa also have high rates of pirated software, compounding difficulties of checking software for malicious components: In 2017, investigations showed 90 percent and 89 percent of software in Libya, Zambia and Zimbabwe, respectively, was pirated (Nir, 2019).
iv. Ineffective law enforcement: As of 2016, 39 of the 54 African countries had no specific legal provisions for cybersecurity and cyber-enabled criminal activity. Furthermore, the lack of cybersecurity specialists means that many states suffer an inability to investigate cybersecurity incidents properly, and weak enforcement mechanisms for the laws that do exist make it harder to identify and arrest perpetrators, effectively making the continent a safe haven for malicious actors to operate with impunity (Joanna, Januray 2020)

1.2 Problem Statement

The Zambian financial industry has changed tremendously thanks to increased trust in digital services and innovations that rely on digital infrastructure. Utility cases have expanded from first-generation services, such as person-to-person transfers, to second-generation services, including merchants and bill payments, microloans, microsavings and microinsurance. The industry is also testing new business models by building partnerships between financial institutions and non-financial institutions, including mobile network operators (MNOs) and financial technology companies (FinTechs). Despite the notable progress recorded, by the end of 2019, only 33% of the population had active DFS accounts on a 90-day period signifying that the majority of Zambians did not have digital financial services accounts (UNCDF, 2019).

The report by the National Assembly of Zambia report on cyber trends in Zambia showed that from January - December 2021, the Zambia Computer Incidence Response Team (ZM-CIRT) recorded a cumulative number of attacks amounting to 10,718,002. The cyber threats recorded in 2021 included: mobile money reversal scams, social media account hijacking and fake online product promotions and investment schemes (National Assembly of Zambia, 2022). Further, the ZICTA report on national cyber risk showed that Zambia is exposed to somewhere between 0.01% and 12.17% of its GDP if a significant cyber-attack affected many organizations for a sustained period. The GDP of Zambia is around $19,320,000,000. The greatest cyber system impacts to GDP would happen from the Banking & Finance sector with a $2,351,244,000 impact with phishing and malware being the greatest weaknesses (ZICTA, 2022).

Falling victim to a scam or experiencing system access errors can result in financial and psychological harm and will most certainly affect a customer’s confidence and trust in the financial service. The negative experiences prove to deter DFS consumers from using mobile money services more frequently and significantly decreased the level of trust in providers and the financial system altogether (Jenny & David , 2022). The trust and confidence in financial service providers (FSPs) and payment systems are key ingredients for sustained financial inclusion, cyber incidents and their associated losses

can hinder efforts to expand access to financial services. Furthermore, these kinds of incidents and customers' negative experiences can spread quickly by word of mouth and may potentially end up splashed across the media. In the wake of such damage, it takes a lot of time and effort to rebuild reputations and people's trust (Njuguna, 2018).

It is evident that despite the important role played by digital financial technologies in enhancing financial inclusion, they have exposed users to cyber threats such as internet scams and fraud. Therefore, this study seeks to analyze the effects that cyber threats on the uptake of digital financial services in Zambia.

1.3 Research Objectives

1.3.1 Main Objective

The general objective of the study is to as analyze the impact of cyber-attacks on the uptake of digital financial services in Zambia**.**

1.3.1.1 Specific objectives

1.3.1.1 To establish which digital financial platforms are available in Zambia and how they are accessed.

1.3.1.2 To Investigate the Types and Causes of Cyber-attacks on Digital Financial Platforms.

1.3.1.3 To assess how secure digital financial platforms are in Zambia.

1.3.1.4 To establish users' perceptions of protection by regulatory authorities against digital financial platforms.

1.4 Research Questions

1.4.3 What digital financial platforms are available in Zambia and how are they accessed?

1.4.4 What are the Types and Causes of Cyber-attacks on Digital Financial Platforms?

1.4.5 How secure digital financial platforms are in Zambia.

1.4.6 What are the users' perceptions of protection by regulatory authorities against digital financial platforms??

1.5 Significance of Study

Our research holds considerable significance in the realm of digital finance and cybersecurity, particularly within the Zambian context. The digital landscape is constantly evolving, and as it does, the importance of ensuring a secure and trustworthy environment for users becomes paramount. Our investigation into the cybersecurity measures for digital financial platforms in Zambia provides insights that are crucial for multiple stakeholders. Here's why our study matters:

1.5.1 Contribution to Knowledge

Firstly, our study stands as a substantial addition to the existing body of literature. While there has been global attention on digital finance, the unique context of Zambia remains underexplored. Our research delves into this very niche, thereby enriching the academic discourse around digital finance and its associated challenges in specific regional settings.

1.5.2 Policy and Regulation Implications

The insights derived from our study have the potential to be instrumental for regulatory bodies in Zambia, including ZICTA. Policymaking thrives on informed perspectives, and our findings can aid in the refinement of existing guidelines and the creation of new, more targeted regulations. As the digital ecosystem in Zambia grows, so does the need for robust and contextually relevant regulatory frameworks.

1.5.3 Promoting Robust Cybersecurity Measures

By highlighting the specific vulnerabilities and challenges that digital financial platform in Zambia encounter, our research offers a roadmap for businesses to amplify their cybersecurity protocols. Understanding where the threats lie and the nature of these threats allows for more effective resource allocation and strategic planning.

1.5.4 Building User Trust

Trust is the cornerstone of any financial system. Our research underscores the areas of concern and potential vulnerabilities, enabling service providers to address these issues head-on. A proactive approach to these challenges, informed by our findings, can foster greater trust and confidence among users.

1.5.5 Economic Growth and Stability

A secure and reliable digital financial environment propels economic growth. Our study indirectly contributes to Zambia's economic stability by shedding light on areas that, when addressed, can lead to higher adoption rates and increased digital financial activities.

1.5.6 Foundation for Future Research

The digital realm is ever-changing. Our findings, while comprehensive, also set the stage for subsequent investigations. We've identified specific areas that might require more in-depth exploration in the future, serving as a foundation for upcoming research endeavours.

1.5.7 User-Centric Awareness

At the heart of any digital platform are its users. Our study, by highlighting the present cybersecurity landscape, serves as an educational tool, empowering users to take informed actions and protect themselves in the digital sphere.

1.6 Scope of study

The study covered sixteen commercial banks with branches in Kitwe, mobile money agents and traders at Chisokone Market in Kitwe and fifteen Microfinances institutions with branch presence in Kitwe.

1.7 key terms of the study

According to this study, key terms include the following and are defined as follows.

i. ***Digital financial service***: this is a financial service/product that can be accessed through the use of internet or SSD codes.

ii. ***Digital financial provider:*** these are companies/ institutions that offer or facilitate for digital financial services like internet banking or mobile money services such as banks and mobile network operators.

iii. ***Cyber threats***: these refer to occurrences or actions caused by cyber criminals that can lead to loss of funds for the users or disruption of digital services.

iv. ***Uptake***: this refers to the use of or access to digital financial services.

v. ***Cybercrime:*** Cybercrime refers to illegal digital actions targeted at users or providers of digital financial services with the aim of stealing money, information or disrupting services.

vi. ***Financial institution:*** in this study, it refers to a company or organization that facilitates or provides financial products such as electronic payment systems.

vii. ***Financial inclusion:*** this refers to how available, accessible, and affordable financial services are to the poor.

viii. ***Unbanked;*** refers to individual with no access to banking or formal financial services.

ix. ***Cyber space:*** refers to digital platform or facility that makes it possible for digital financial transactions to take place.

1.8 Thesis Outline

Chapter 1: Introduction

The introduction serves as the foundation for the entire thesis, providing a broad overview of the research topic. This chapter highlights the significance of studying the cybersecurity measures in place for digital financial platforms in Zambia. The reader is introduced to the background of the study, shedding light on the increasing importance of digital financial platforms in Zambia and the accompanying cyber threats. Clear objectives are set out, which guide the subsequent research.

Chapter 2: Literature Review

Delving into existing academic and industry literature, this chapter offers a comprehensive overview of digital financial platforms available globally and, more specifically, in Zambia. The various types of cyber threats that these platforms face are detailed, as well as the prevailing cybersecurity measures in place. The chapter underscores the gap in literature, particularly in the context of Zambia, justifying the need for the current study.

Chapter 3: Methodology

Detailing the blueprint of the research, this chapter provides an insight into how the study was carried out. From the sampling methods to the data collection tools, every technique and instrument used in the study is described. The target population of traders, mobile money agents, and digital financial providers is specified. Ethical considerations and potential limitations of the study are also candidly discussed, ensuring transparency in the research process.

Chapter 4: Data Analysis and Results

The collected data is presented and analysed in this chapter. Through tables, charts, and descriptive statistics, the reader gets a clear picture of the digital financial landscape in Zambia. Key findings related to the type of digital platforms, user numbers, and reported cyber-attacks are highlighted. Each table and figure are accompanied by a narrative interpretation, ensuring that the data speaks to the objectives set out in the first chapter.

Chapter 5: Discussions and Findings

Building on the results presented in the previous chapter, this segment delves deeper into interpreting the findings in the context of existing literature and the study's objectives. Each objective is discussed in detail, juxtaposing the study's results with findings from other research. This chapter synthesizes the results, offering a holistic understanding of the cybersecurity dynamics of digital financial platforms in Zambia.

Chapter 6: Recommendations and Future Research

Concluding the thesis, this chapter provides actionable recommendations based on the research findings. These suggestions are aimed at digital financial providers, regulatory authorities, and end-users, ensuring a multi-pronged approach to enhancing cybersecurity. A section dedicated to future research offers directions for upcoming researchers, pointing out areas that could benefit from further exploration.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

In this chapter, the researcher presents the review of the published literature related to the study. The review focuses on the overview of digital finance, cyber threats and relevant theories based on past studies that have been undertaken by scholars on similar/related research topics/study.

Peake (2012) defines digital finance as the delivery of financial services through digital channels such as internet, computers, and mobile phones. On the other hand, the World Bank (2015), defines digital finance as the computerized administration of financial services through the utilization of advanced innovations (web, versatile correspondence innovation) and facilitates the payment exchanges. In a nutshell, digital financial services generally refer to the far-reaching technologies available to perform financial services from a widespread range of providers to different categories of users. This is made possible through the use of digital remote means including e-money, mobile money, card payments, and electronic funds transfers (IMF, 2021). furthermore, Niamh 2016 expounds that computerized Financial Services (DFS) are basically about sparing cash, getting to credit and protection, and performing exchanges through advanced channels like cell telephones, cards, PCs, tablets, et cetera (Niamh, 2016). Digital financial payment products allow users to access funds from far-flung businesspeople, relatives, and friends during moments of crisis, reducing the likelihood that they will fall into poverty (Niamh, 2016). Advanced budgetary administrations, for example, versatile cash furnish people with more prominent accommodation, protection, and, as a rule, improved security contrasted with putting away money at home or going with money (IMF, 2021).

(Park & Mercado, 2018) estimated that about two billion adults have no access to formal financial services worldwide. Such figures have led to growing recognition of the need to go beyond general consideration of financial sector development and to pay particular attention to financial inclusion. This is consistent with a general shift in global

development thinking away from the neoclassical Washington Consensus that, among other things, espoused the “trickle down” effect, and towards broad-based and inclusive strategies. Such strategies are well-articulated in the United Nations’ 2030 Agenda that provides a framework for implementing the Sustainable Development Goals (SDGs) through a commitment to ensuring “no one will be left behind (UDNP, 2018)

The World Bank in their 2020 study on digital indicated that the Covid-19 pandemic had demonstrated even more the need and benefits of expanding digital financial services. This is because digital finance significantly reduces the need for physical contact in retail and financial transactions and helps government respond more quickly to extend liquidity to firms and people most at risk. Particularly through the use of mobile money, digital financial channels allow remote payments and transactions, enabling the social distancing recommended to reduce the further transmission of the pandemic. Through electronic payments, consumers can transfer funds, pay bills and pay for goods and services from their home, or in a market or store setting, with limited physical contact. Finally, digital financial services enable a rapid, secure way for governments to reach vulnerable people with social transfers and other forms of financial assistance, especially during times when transportation and movement around the country is unsafe or limited (World Bank Group, 2020).

According to Maurer and Nelson 2021, two ongoing trends increase cyber risk. Firstly, they point to the global financial system which they say was undergoing through an unprecedented digital transformation, which of course was being accelerated by the COVID-19 pandemic. This has created a situation where banks compete with technology companies and vice versa. Meanwhile, the pandemic has heightened demand for online financial services. Central banks around the globe are considering throwing their weight behind digital currencies and modernizing payment systems. In this time of transformation, when an incident could easily undermine trust and derail such innovations, cybersecurity is more essential than ever. Secondly, cyber criminals are taking advantage of this digital transformation and pose a growing threat not only to the global financial system but also to the financial stability and confidence in the integrity of the system. The pandemic has even supplied fresh targets for hackers. The financial

sector is experiencing the second-largest share of COVID-19–related cyberattacks, behind only the health sector, according to the Bank for International Settlements (Maurer & Nelson, 2021).

2.1 Empirical Review

2.1.1 Digital Financial Platforms

Digital financial platforms have become ubiquitous in many parts of the world, signifying a pivotal transformation in the way monetary transactions are conducted. According to Radcliffe and Voorhies (2022), nearly two-thirds of the unbanked population globally now have a mobile device, positioning digital financial services as a potential remedy to the challenge of financial inclusion. Meanwhile, Kharas and Dooley (2021) argue that these platforms have been instrumental in bolstering economic growth, enhancing the efficiency of transactions, and fostering financial resilience, especially in developing countries. However, a counterview presented by Turner et al. (2023) suggests that while the platforms offer numerous benefits, they also expose users to cyber threats and data privacy issues. This dichotomy indicates that while digital financial platforms have indeed revolutionized financial services globally, there is an impending need for tighter security and regulatory mechanisms.

In Africa, digital finance has witnessed an unparalleled surge. Mbiti and Weil (2022) noted that mobile money, a form of digital financial platform, has grown rapidly in many African nations, becoming a primary means of transaction for millions. It has especially played a pivotal role in regions where traditional banking infrastructures are sparse. Yet, Aker and Mbiti (2021) shed light on the disparities within the continent, where countries like Kenya and Ghana are far ahead in adoption compared to nations like Chad and Central African Republic. Nguena and Abimbola (2023) raised concerns over the regulatory environments, emphasizing the lack of a unified framework to oversee and guide these platforms' operations in various African nations. Their research suggests that while the adoption is promising, the continent must address regulatory disparities to ensure sustainable growth.

In Zambia, the narrative around digital financial platforms mirrors much of the broader African experience but with specific nuances. Tembo and Mulenga (2021) have highlighted how these platforms, especially mobile money, have democratized access to financial services in the country. However, Lungu and Phiri (2022) point out that with the rise in the use of digital platforms, Zambia has also witnessed an uptick in cyber fraud incidents, signifying the dark underbelly of this digital revolution. There is a growing call, notably from Banda and Chanda (2023), for a more robust regulatory framework that is not only responsive to the evolving digital landscape but also places a premium on user protection and data privacy.

While the benefits of digital financial platforms are evident, the associated risks cannot be downplayed. The international perspective reveals a promising trajectory, but as the African and Zambian perspectives indicate, regional nuances play a significant role. It is essential for stakeholders, from policymakers to service providers, to adopt a balanced approach – one that promotes innovation while ensuring security and trustworthiness.

2.1.2 Cyber-attacks on Digital Financial Platforms

The onset of digital financial platforms has inadvertently opened Pandora's box of cyber threats on a global scale. Martinez and Alonso (2022) categorize these threats into several key types: phishing, malware attacks, Distributed Denial of Service (DDoS) attacks, and man-in-the-middle attacks. These attacks primarily exploit vulnerabilities in software, human error, and inadequate infrastructure. Cerny and Fischer (2021) emphasize that the consequences of such attacks are not merely financial losses but also loss of consumer trust, brand reputation damage, and potential regulatory penalties. From the global vantage, there is a glaring need for continuous monitoring and adaptive countermeasures to keep pace with evolving cyber threats.

Digital finance in Africa, although revolutionary, is accompanied by a growing vulnerability to cyber-attacks. Okafor and Adebanjo (2023) note that Africa's rapid digital financial adoption has, in many instances, outpaced the development of adequate cybersecurity measures. They have identified mobile-based malware and SMS phishing as

predominant attack vectors, largely fueled by low digital literacy among the populace. Adedeji and Olugbara (2022) discuss the severe aftermath of such attacks in the African context, including financial losses, reduced faith in digital platforms, and even potential sociopolitical implications given the scale of reliance on these platforms for daily transactions.

In Zambia, as digital financial platforms gain traction, so does the frequency and sophistication of cyber-attacks. Chikoti and Sichone (2021) note a concerning rise in malware attacks targeting mobile banking apps. They attribute the rise to weak application security measures and users' lack of awareness about secure online behaviors. Mwamba and Nkole (2023) delve into the ramifications of these attacks, asserting that beyond immediate financial repercussions, there is a lingering impact on the country's overall digital financial ecosystem's growth and trustworthiness.

Cyber-attacks on digital financial platforms remain one of the most pressing challenges of the digital age. While the international and regional perspectives offer a clear picture of the widespread nature of the problem, localized insights, like those from Zambia, underscore the importance of tailored solutions. It is imperative for regulators, financial institutions, and tech developers to collaboratively advance both technology and user education to curb this digital menace effectively.

2.1.3 The Security of Digital Financial Platforms

Globally, there is an ongoing debate regarding the security of digital financial platforms. In a study by Ivanova and Petrov (2022), it is posited that most international banking and financial institutions maintain rigorous security protocols. This includes encryption techniques, two-factor authentication, and regular security audits. However, Roth and Schmidt (2021) argue that despite these measures, digital financial platforms remain vulnerable, primarily because cybercriminals continue to evolve their techniques in tandem with or sometimes even ahead of security advancements.

The African context offers a mixed bag when it comes to the security of digital financial platforms. Due to rapid digitization without parallel advances in cybersecurity, many

platforms are more susceptible to breaches. As documented by Ngugi and Mureithi (2023), many African countries have shown a rise in successful cyber-attacks on digital banking and payment systems. However, on the brighter side, institutions are taking cognizance. Akande and Uche (2022) detail efforts, especially in larger economies like Nigeria and South Africa, where financial technology startups and traditional banks are heavily investing in advanced security infrastructure and public cybersecurity education.

In Zambia, digital financial platforms have seen an upward trajectory in both adoption and security measures. Chanda and Bwalya (2021) provide insights into the Zambian digital financial landscape, noting that while earlier platforms had security vulnerabilities, newer systems are increasingly adopting international security standards. Mweemba and Phiri (2023) echo this sentiment but also caution that user awareness and education lag, often becoming the weak link in the security chain.

Ensuring the security of digital financial platforms is a continuous and dynamic challenge. No singular solution can guarantee protection, and it is a combination of technology, regulations, and user awareness that can together fortify these platforms. While international and African perspectives highlight various challenges and measures, the Zambian scenario exemplifies a classic case where technological advancements need to be complemented with user-centric measures for a holistic security framework.

2.1.4 Protection of Users on Digital Financial Platforms by Regulatory Authorities

Globally, regulatory authorities have been at the forefront of ensuring that users of digital financial platforms are safeguarded against potential risks. According to Martinez and de la Rosa (2022), many countries have implemented stringent regulations that mandate platforms to adhere to international security standards, employ encryption techniques, and undergo periodic audits. Nevertheless, Garcia and Ortiz (2021) highlight a notable challenge: while regulations are present, their enforcement remains inconsistent, leading to disparities in user protection across various regions.

The African regulatory landscape regarding digital financial platforms is evolving. Olufemi and Adebayo (2023) note that while many African nations recognize the imperative need

for robust regulations, implementation remains staggered due to diverse economic, political, and technological environments across countries. Notably, countries like Kenya and Rwanda have made significant strides with their regulatory frameworks, ensuring user protection on digital platforms. Yet, as observed by Kibet and Muchiri (2022), some regions still lag, leaving users vulnerable to potential financial threats.

In Zambia, the protection of users on digital financial platforms by regulatory bodies has garnered significant attention. Studies by Sikazwe and Tembo (2021) underscore the proactive approach adopted by the Zambian authorities. Regulatory frameworks have been revised periodically to incorporate the evolving nature of digital finance and associated risks. However, Lungu and Chileshe (2023) point out that while regulations exist, user awareness about these protections remains relatively low, indicating a need for more significant outreach and education.

Regulatory authorities play a pivotal role in ensuring the safety of users on digital financial platforms. While regulations themselves are essential, their consistent enforcement and periodic updating, in tandem with the rapidly changing digital finance landscape, are equally crucial. International and African perspectives elucidate the challenges and achievements in this arena. The Zambian experience serves as an exemplary model, highlighting the importance of not just having regulations in place but also ensuring that users are aware of and can leverage these protections.

2.2 Theoretical Framework

2.2.1 Technology Acceptance Model

In 1986 Davis forwarded this model in a bid to explain the behavior behind the urge to employ technological know-how. (David, 2020). The TAM does not deal with systems but rather it deals with fourteen perceptions and it contends that when new technological advancement is introduced to the customers, either one of this occurs that is, Perceived Ease of Use (PEOU) and Perceived Usefulness (PU) influence their decision (Douglas & Loader, 2020). PEOU is the level of confidence that people put on a system and if users perceive a new technology to be beneficial in support of both short and long-run, there is that encouragement to use the system. Further, the level by which an individual considers a system will boost performance in the short and long-run is the PU (Jenny & David , 2022). The TAM affirms that the system's real utilization is established by each user's behavioral intention for usage and is inspired by an individual's perception to the system. The theory also explains that the perception towards new technology has a direct relation to its functionality as well as the simplicity of the system (Douglas & Loader, 2020). TAM considers that acceptance of technology and functionality is influenced by consumer's intentions that establish the customer's perception towards system (Douglas & Loader, 2020).

The theory also supports that the recognitions or suspicions about the advancement are instrumental in the improvement of states of mind that will in the long run result in system usage conduct (Douglas & Loader, 2020). TAM also explores the attitude of individuals towards particular system (Salah, Maureen, & Cameron, January, 2022). The TAM gives details and clarifies and portrays the reasons why clients acknowledge or dismiss an advancement or data framework. TAM is important both as a prescient strategy, considering the objective to evaluate the probability of individuals and associations to receive a specific innovation (Jenny & David , 2022). TAM can be used to explain the digital financial services which can be applied in clarifying the 15 existences of variations in consumer behaviors especially when it comes to use of related digital financial services (Silvia, Judith, & David, 2019).

2.2.2 Theory of Financial Innovations

The theory of financial innovations was proposed by Silber (1983) premised on the idea that benefits from expansion of money related foundations is the key reason of financial inclusion (Silvia, Judith, & David, 2019). The theory demonstrates that the primary thoughts behind the new innovations are the defects of the money related business sector, mostly the deviated data, office expenses and exchange costs (Joanna, Januray 2020). According to the theory, financial related innovations can be very new resolutions or simply customary means whereby latest component of development has been offered, enhancing firms' liquidity as well as expanding quantity new applicants, due to their qualifications on the situation (Jenny & David , 2022). Furthermore, according to this theory, financial innovation is a critical motivating force of the financial system, which leads to better economic competence and enhanced economic advantage derived from the new and frequent changes (Niamh, 2016). Financial innovations define financial developments by coming up with new ways of production, technological solutions, creating better return rates, hence boosting the country's economy in general. The theory stresses that the innovativeness improves the firms' competitive edge of a corporate and generates more earnings to the investors (Nir, 2019).

Innovation is a tool used to solve, manage, and transfer the entire extra burden. The application of innovations promotes growth of financial entities through improved allocation, efficiency, and a reduction of financial and administration costs (Park & Mercado, 2018). Financial innovations enhance financial markets liquidity and ensure the allocation of resources to insufficient areas as well as improving the accessibility to emerging prospects (Nir, 2019) hence deepening financial inclusion. The theory of financial innovations reiterates that some restrictions including external handicaps helps corporations in their pursuit of their objective which is maximization of revenues (Jenny & David , 2022) hence commercial banks come up with innovative ways to reach more people to improve their profits. The emerging innovative financial inclusion models through mobile and other digital financial services especially in many African countries which are assisting in closing the gap of financial instruments which exists in these countries (Wechsler & Siwakoti, 2018).

2.2.3 The dissatisfaction theory of financial inclusion

The dissatisfaction theory of financial inclusion argues that financial inclusion programs in a country should first be targeted to all individuals who were previously in the formal financial sector but left the formal financial sector because they were dissatisfied with the rules of engagement in the formal financial sector, or had some unpleasant personal experience when dealing with firms and agents in the formal financial sector.6 This theory suggests that it is easier to bring back people who left the formal financial sector because they were dissatisfied if the areas of dissatisfaction in the formal financial sectors have been completely resolved. According to this theory, it is simpler to persuade this set of people to return to the formal financial sector than it is to introduce them to those who have never worked in it. This idea implies that financial inclusion programmes should prioritize serving the people that departed from the formal financial system before expanding to include other segments of the population. Adults who have a bank account may experience dissatisfaction for a variety of reasons, including financial fraud, debit or credit card fraud, theft, lengthy wait times before depositors can withdraw their money, lengthy payment processing times, exorbitant transaction fees, unjustified bank charges, etc.

2.2.4 The Rational Choice Theory (RCT)

Another name for this framework, which is frequently used to formally explain social and economic behavior, is the rational action theory. Furthermore, the theory places a lot of emphasis on the factors that influence each person's decision. According to the RCT, people are typically motivated to participate in anything by their preferences and aspirations. Individuals' activities are mainly controlled by knowledge of the circumstances that humans face when trying to accomplish their goals. More importantly, RCT can benefit from the application of the same economic theories' tenets, which facilitate understanding the exchange of resources like status and time among many others. Generally speaking, fulfilling human desire is difficult. An important domain RCT can be goals selected in a way that meets the established targets. According to Scott (2000), each and every human being must be able to comprehend the reasons behind their own goal setting and be aware of the consequences of that decision. Essentially,

almost all microeconomic analysis in the RCT is based on human decision making. The conventional definition of rational choice is the process of ascertaining the options that are available and then selecting the option that is most favored based on a consistent criterion. This rational choice model is already, in a way, an optimization-based method. Thus, the purpose of this study is to determine whether cyberthreats are influencing Zambia's adoption of DFS. Users of DFS will apply rational computations to make logical decisions and attain results that are consistent with their own personal goals, according to the rational choice theory. This hypothesis will be used in the study, but it will be dependent on the individual choices made by participants to use digital financial services. This means that, given the options accessible to them, applying this theory will provide results that maximize people's benefit and enjoyment.

2.2 Conceptual Framework

This conceptual framework shows the relationship between the independent variable which is cyber security and the dependent variable uptake of digital financial services.

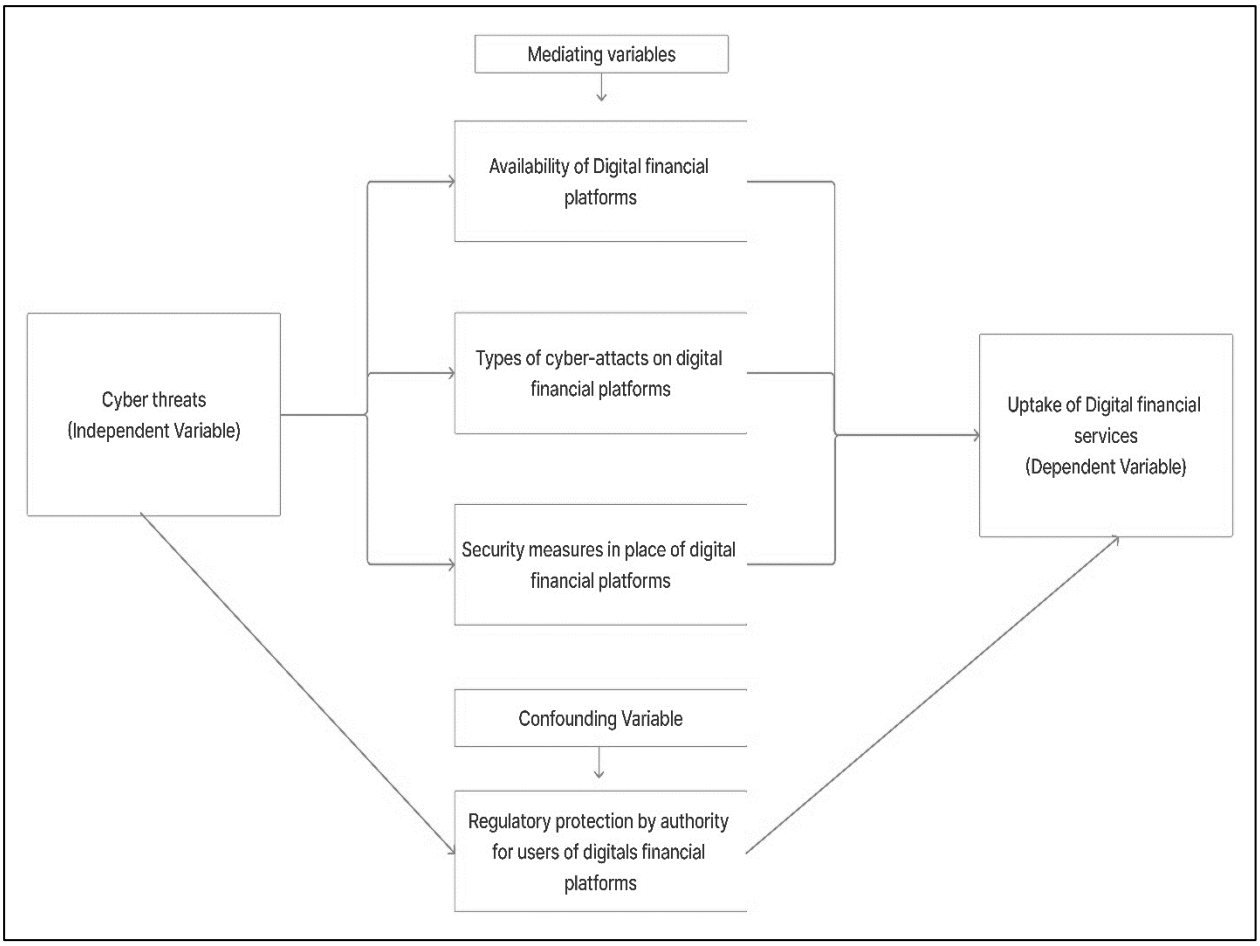

Figure 1: Conceptual framework for the study on the effects of cyber threats on the uptake of digital financial services in Kitwe. (Adapted from Martinez,2022)

2.3.1 Availability of Digital Financial Platforms

The availability of digital financial platforms pertained to the array of digital financial services and platforms that were operational and accessible in Zambia during the period of study.

To gauge the availability of these platforms, a two-pronged approach was adopted. Initially, a comprehensive literature review was conducted to identify the major players and the niche digital financial solutions in Zambia. The literature served as a preliminary source, giving a bird's-eye view of the digital financial landscape in Zambia. This review considered articles, whitepapers, industry reports, and publications from financial institutions, regulatory bodies, and technology agencies.

Subsequently, primary data was collected using surveys. These surveys targeted two distinct groups: end-users and service providers of digital financial platforms. For the end-users, the survey aimed to ascertain which platforms they were aware of, which ones they actively used, and the frequency of usage. This helped in understanding the ground reality of platform availability from a user's perspective.

On the other hand, service providers were surveyed to gather a more holistic understanding of the platforms they offer, their user base size, and any other platforms they were aware of but did not directly provide. Interestingly, the survey incorporated a mix of structured questions, listing known platforms, and open-ended queries. The open-ended options were particularly enlightening, as they enabled respondents to mention emerging or less-known platforms that might not have been extensively covered in the literature.

The synthesis of findings from both the literature review and the surveys provided a robust answer to research question 1.4.1. Through this combined approach, not only was the spectrum of available digital financial platforms in Zambia mapped out, but insights into their popularity, user preference, and market reach were also gleaned.

2.3.2 Types of Cyber-attacks on Digital Financial Platforms

The term "types of cyber-attacks on digital financial platforms" encompasses the various techniques and methods malicious actors employed to compromise the integrity, confidentiality, or availability of digital financial services and platforms accessible to Zambians during the research period. To determine the range and nature of these cyber-attacks, an integrated approach was taken:

1. **Literature Review**: A comprehensive review of academic journals, industry reports, and cybersecurity publications provided an overview of the most prevalent cyber-attacks on digital financial platforms globally, within Africa, and specifically in Zambia. This literature review served as a foundational tool, offering a theoretical understanding of the threat landscape in the digital finance domain.

2. **Surveys**: Customized questionnaires were designed for two distinct demographic groups: end-users of digital financial platforms and the platforms' service providers.

    - **End-users Survey**: This aimed to capture users' experiences with cyber threats. Questions revolved around their awareness of cyber-attacks, personal experiences of security breaches, and the perceived vulnerability of the platforms they use.

    - **Service Providers Survey**: Digital financial platform providers were questioned about the types of cyber-attacks they have encountered, their frequency, mitigation measures in place, and the overall impact of these attacks on their operations. It was vital to get this insider's perspective because service providers would be privy to technical details and backend threats that end-users might not be aware of.

3. **Open-ended Questions**: In both surveys, respondents were encouraged to detail their experiences or knowledge of cyber-attacks that might not fall into commonly recognized categories. These open-ended responses offered rich, qualitative data, shedding light on emerging or unique threat vectors.

By combining insights from scholarly articles with firsthand accounts from surveys, the research offered a multi-dimensional understanding of the types of cyber-attacks targeting digital financial platforms in Zambia. This methodical approach ensured that research question 1.4.2 was thoroughly addressed, presenting both a macro and micro perspective on the cybersecurity challenges faced by the Zambian digital finance sector.

2.3.3 Security Measures in Place for Digital Financial Platforms

The term "security measures in place for digital financial platforms" encapsulates the diverse preventive, detective, and corrective mechanisms that digital financial service providers employ to shield their platforms and users from cyber threats. These measures may range from multi-layered authentication processes, end-to-end encryption, continuous security audits, to advanced threat intelligence systems.

Testing Method: To gain a comprehensive understanding of the robustness and comprehensiveness of these security measures:

1. **Literature Review**: Scholarly articles, industry standards, and global best practices were reviewed to understand the benchmark security measures that digital financial platforms should ideally adopt.

2. **Surveys with Service Providers**: Customized questionnaires aimed at service providers would inquire about the nature and depth of security measures they've instituted. Questions would cover topics from user data protection, transaction security, to backend infrastructure safeguards.

3. **Penetration Testing**: With the consent of digital financial service providers, ethical hacking or penetration testing would be conducted. This would give a hands-on assessment of how resilient the platform's defenses are against simulated cyber-attacks. Such tests often reveal vulnerabilities that might not be apparent through self-reporting by platforms.

2.3.4 Regulatory Protection by Authorities for Users of Digital Financial Platforms

Definition

Regulatory protection by authorities" refers to the official statutes, guidelines, and supervisory practices that governmental or regulatory entities have institutionalized to safeguard the rights, data, and funds of users on digital financial platforms.

Testing Method:

1. **Policy and Regulation Review**: All relevant governmental and regulatory body documents would be perused to derive an understanding of the regulatory landscape. This would encompass laws, directives, and guidelines that pertain to the operation and security of digital financial platforms.

2. **Surveys with End-users**: To gauge the user perspective on regulatory protection, surveys were conducted to discern their awareness of their rights, their

experiences in seeking redress or support, and their perceptions of the efficacy of regulatory bodies.

3. **Feedback from Digital Financial Providers**: Providers would be asked about their experiences in complying with regulations, the challenges they face, the support they receive from regulators, and their suggestions for regulatory improvement.

By amalgamating insights from both the creators and the subjects of these regulations, this multifaceted method illuminated the practical effectiveness and potential gaps in the regulatory framework safeguarding digital financial platforms in Zambia. This comprehensive approach was geared towards addressing research question 1.4.4.

CHAPTER THREE

RESEARCH METHODOLOGY

3.0 Introduction

This chapter details how the research was conducted and analysed. The chapter describes the research design, population, sample and sampling technique, data collection methods, data collections procedure, data processing and analysis.

3.1 Research Approach

When considering the research approach for a study focusing on the digital financial landscape, particularly in areas such as cybersecurity threats and user experiences, a quantitative approach is often advantageous. This method allows for the collection and analysis of numerical data, providing a more objective basis to draw conclusions and identify patterns or trends.

A quantitative approach was particularly suited for assessing the prevalence and types of cyber-attacks on digital financial platforms, as it enabled the researcher to quantify the incidence rate of various cyber threats and analyze correlations with potential causative factors. For instance, statistical analyses can reveal whether certain demographic groups or platform types are more susceptible to specific kinds of cyber-attacks, thus offering concrete data to back policy or security enhancement recommendations (Creswell, 2014).

Furthermore, quantitative methods facilitated the evaluation of user confidence in digital financial platforms and regulatory measures' effectiveness. Through structured surveys and questionnaires, researchers can gather data on users' perceptions and experiences, allowing for the numerical assessment of user satisfaction and trust levels. Such data is invaluable for regulatory bodies and service providers aiming to identify areas for improvement (Bryman, 2016).

Choosing a quantitative approach also allowed for the potential application of predictive models to forecast future trends in cyber threats or user behavior, contributing to more proactive measures in enhancing the security and usability of digital financial services (Field, 2013).

However, it's essential to acknowledge that while quantitative methods offer many benefits, they may not capture the nuanced understanding of user experiences and motivations that qualitative methods can provide. A mixed-methods approach, combining quantitative and qualitative data, could offer a more comprehensive overview, though it would require more resources and complex analysis (Creswell & Creswell, 2017).

3.1.1 Research Design

The descriptive research design was particularly suited for this study due to its strength in facilitating an in-depth exploration of complex phenomena within their real-life context. By focusing on a descriptive, the research can delve deeply into the experiences, perceptions, and behaviors of individuals within the digital financial ecosystem, providing rich, detailed insights that are often not achievable through other designs. This approach allowed for an examination of the nuanced interactions between users, technology, and regulatory frameworks, offering a comprehensive understanding of the factors influencing the adoption and use of digital financial services. Furthermore, the descriptive study design is conducive to integrating both quantitative and qualitative data, enabling a multifaceted analysis of the research problem (Yin, 2018).

3.2 Target Population

The target is about 600 traders who use DFS. The decision to focus on 600 frequent users of digital financial platforms was grounded in the need to capture a wide array of user experiences and interactions with these platforms. Frequent users are likely to have a deeper understanding and more nuanced perspectives on the platforms' functionality, security measures, and potential areas for improvement. This population size was substantial enough to ensure variability in user experiences while manageable for in-depth analysis. Focusing on frequent users also increased the likelihood of gathering

insights on cybersecurity threats, as they are potentially more exposed to such risks due to their higher activity levels on these platforms (Babbie, 2016).

3.3 Sampling Procedure

The sample size of 300, comprising users, employees, and digital financial providers, was selected to provide a comprehensive overview of the digital financial ecosystem from multiple vantage points. This size represented 50% of the defined population, offering a statistically significant subset for analysis while ensuring diversity within the sample. Including employees and providers in the sample is crucial as they offer insider perspectives on the operational, technical, and strategic aspects of digital financial services, complementing the user viewpoints. This balanced approach facilitated a holistic understanding of the digital financial landscape, encompassing both the consumer experience and the operational challenges and opportunities (Creswell, 2014).

3.4 Data Collection Instruments

The instruments employed in data collection are semi-structured questionnaires) which will be given to the respondents. The questionnaires will be administered to traders at the targeted market. The questions contained in these data collection instruments were both open-ended and closed-ended. Such a design made it possible for the collection of both types of data, qualitative and quantitative data.

The open-ended questions allowed respondents to express their views about certain items as these questions allowed for diverse views from respondents and because of this, they were of great importance in coming up with valid findings that reflected one's true views. However, after collecting data, the open-ended questions were coded and eventually closed. Questionnaires were used because they can be used to collect large amounts of data from a large number of people within the shortest possible time and the other justification is that they were a cheaper way of collecting data.

3.5 Data Analysis Techniques

Quantitative data collected from the semi-structured questionnaires were analysed by the use of computer software known as Statistical Package for Social Science (SPSS). This

method grouped the data and presented it in the form of tables, graphs, and charts among others. Open-ended questions in the questionnaires were analyzed using the same software and this was done after closing the responses as well as coding them. The reason for using SPSS was that it is a comprehensive and flexible statistical analysis and data management software program that allows for simple creation of frequency tables, descriptive statistics, exploratory statistics, and cross-tabulation tables. Statistical Package for Social Sciences is a user-friendly Software that is capable of automatically converting data into percentages and other statistical interpretations and easier to analyse the different variables involved and assess their effect on each other.

3.6 Limitations to the Study

Some of the challenges that I experienced in my research was financial and transport constraints, coupled with lack of enough data by the respondents in the field during data collection. However, effective measures were taken to ensure that the challenges were addressed.

3.7 Ethical Considerations

Several ethical considerations were taken into account throughout this study:

1. **Informed Consent:** All participants were informed about the nature and purpose of the study, their participation was entirely voluntary, and they had the right to withdraw at any time without any consequences.

2. **Confidentiality and Privacy:** All information collected from the participants was kept strictly confidential. The data was anonymized and stored securely to ensure that participants' identities were not disclosed.

3. **Honesty and Integrity:** The research was conducted in an honest and transparent manner. Any biases, conflicts of interest, or limitations were openly acknowledged. There was no manipulation or misrepresentation of data.

4. **Respect for Participants:** Participants' rights, dignity, and diversity were respected at all times. Any feedback or complaints from participants were taken seriously and addressed promptly.

5. **Risk and Benefit Assessment:** The potential benefits of the study were weighed against any potential risks or discomfort to the participants. Efforts were made to minimize any risks and to ensure that the benefits of the study were shared with the participants, such as through providing them with a summary of the research findings.

3.8 Limitations of the Study

Despite the rigorous design and implementation, this study has several limitations:

1. **Limited Sample Size:** The study was conducted among traders and mobile money agents at Chisokene Market and representatives of digital financial service providers in Zambia. While efforts were made to select a representative sample, the findings might not be generalizable to all users and providers of digital financial platforms in Zambia.

2. **Subjective Responses:** The study relied heavily on self-reported data, which can be subject to biases, such as social desirability bias and recall bias.

3. **Cross-sectional Design:** The study used a cross-sectional design, which provides a snapshot of the situation at a specific point in time. This design does not allow for tracking changes over time or establishing causality.

4. **Potential Response Bias:** There might be potential response bias, as those who have had negative experiences might be more likely to participate in the study.

5. **Cybersecurity Complexity:** Cybersecurity is a complex, rapidly evolving field. While this study has attempted to provide an overview of the situation in Zambia, it might not capture all the nuances and intricacies of cybersecurity in digital financial platforms.

These limitations were acknowledged and taken into account in the interpretation and generalization of the study findings. Future research can address these limitations by using larger and more diverse samples, longitudinal designs, and more objective measures of cybersecurity.

CHAPTER FOUR

DATA ANALYSIS

4.0 Introduction

In this chapter, i delved into the heart of our research study by examining and interpreting the data collected. The primary purpose of this data analysis was to understand the current state of digital financial platforms in Zambia, the prevalent cyber threats they encounter, the security measures in place, and the role of regulatory authorities in ensuring user safety.

The data collected through surveys from both the end-users and digital financial providers was subjected to thorough quantitative analysis, focusing on frequencies, percentages, and correlations. Additionally, the study also sought to interpret descriptive statistics such as range, mode, minimum, and maximum values.

This chapter begins with an examination of demographic data, including the type of organisations involved, the digital financial services they offer, and the range of users they serve. Following this, explored data pertaining to the occurrence and type of cyber-attacks, the security measures in place, and the perceived effectiveness of these measures.

4.1 Demographic Analysis (Digital financial users)

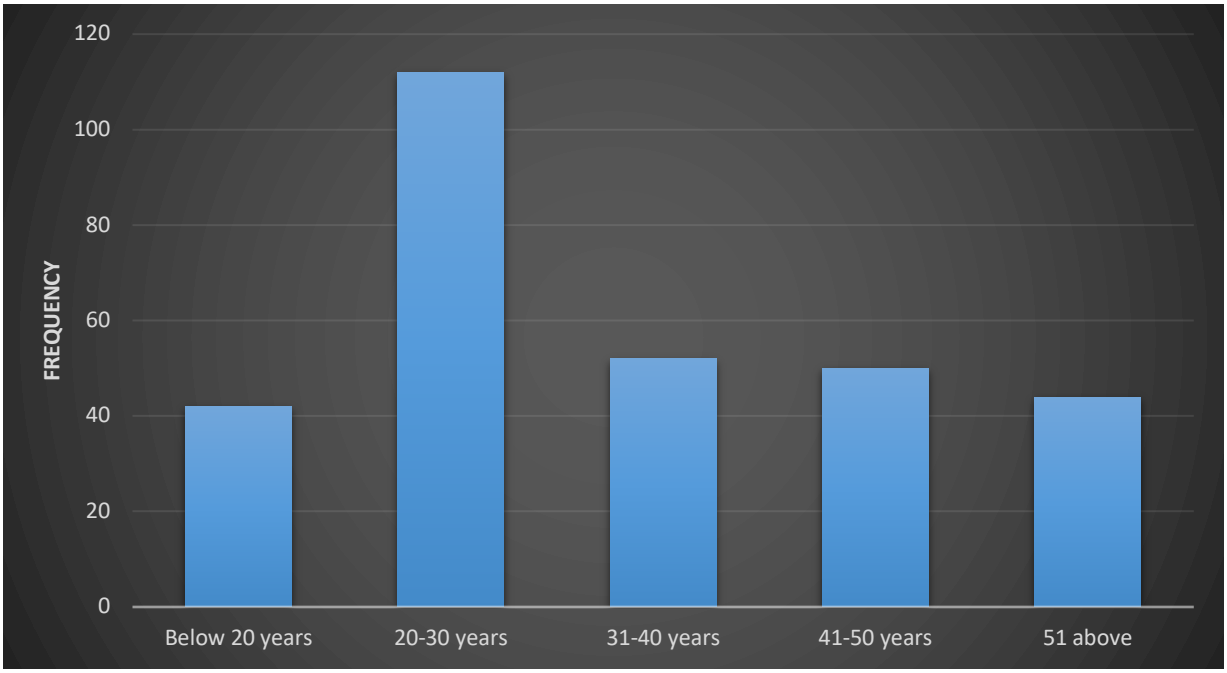

Figure 1: Age

In terms of age distribution, the majority of the respondents (37.3%) are within the age bracket of 20-30 years. This is followed by the 31-40 years age group which represents 17.3% of the population, the 41-50 years group making up 16.7%, and those above 51 years at 14.7%. The least represented age group is those below 20 years at 14%.

4.1.1 Gender

Regarding gender, the population consists of more males (65.7%) than females (34.3%), reflecting a male-dominant environment within the market.

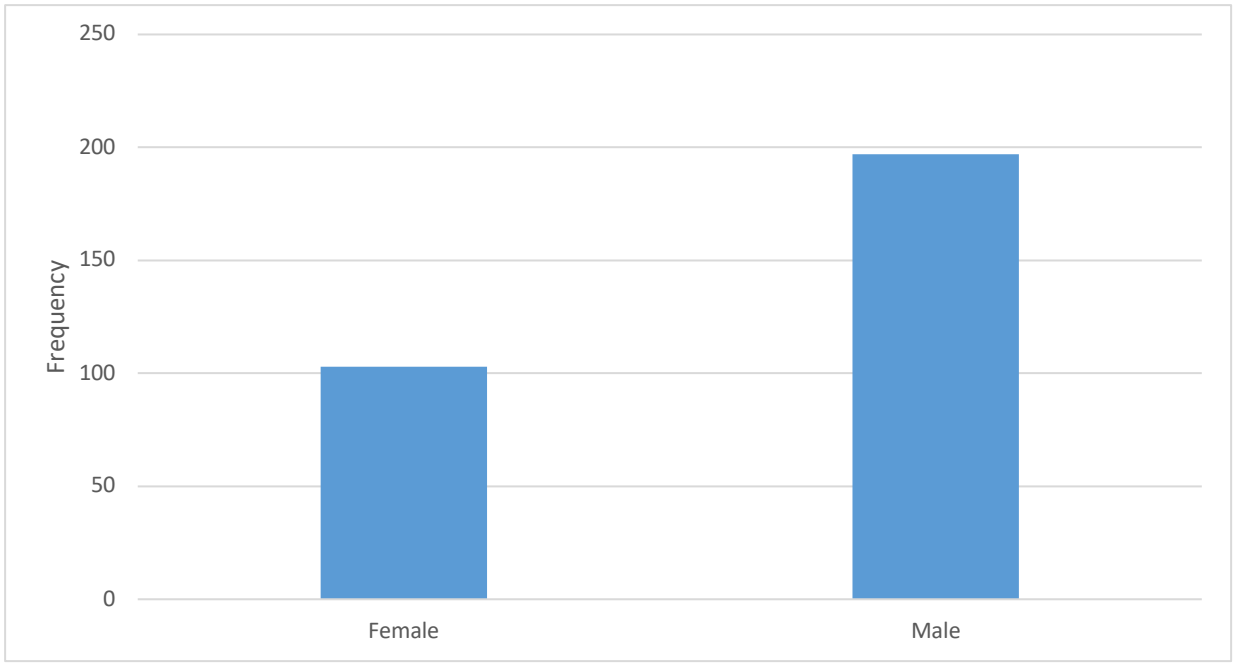

Figure 2:Gender

4.1.2 Roles in the Market

For their roles in the market, most respondents identified as mobile money agents (47%), followed by traders (39.7%), with a smaller percentage (13.3%) engaging in both roles.

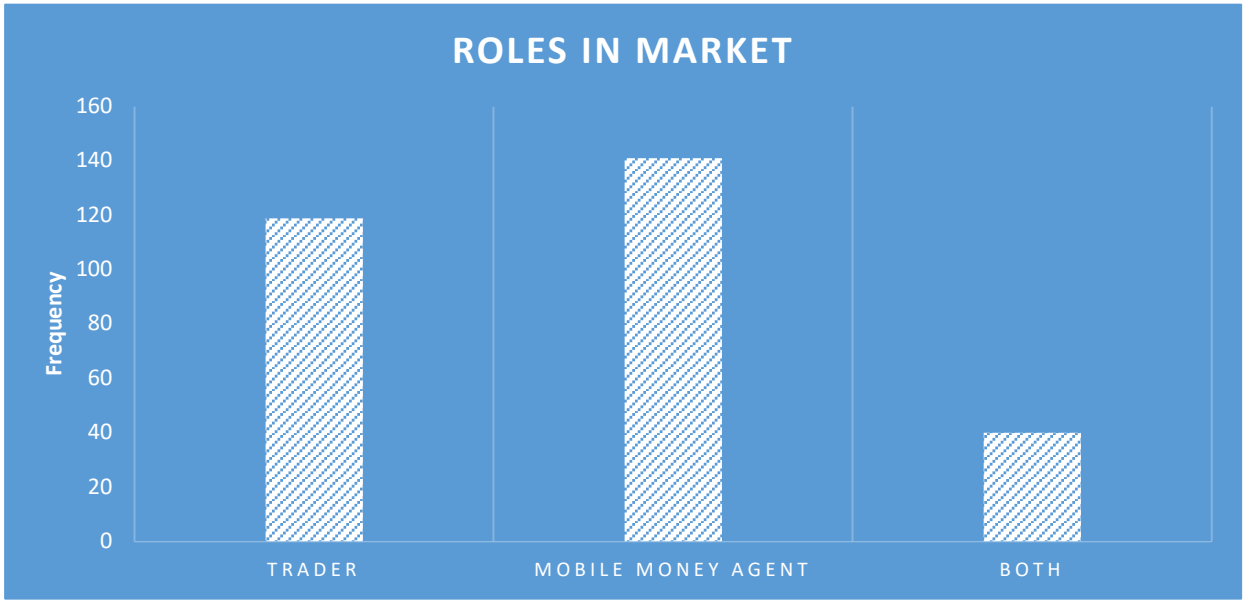

Figure 3:Role in market

4.1.3 Education

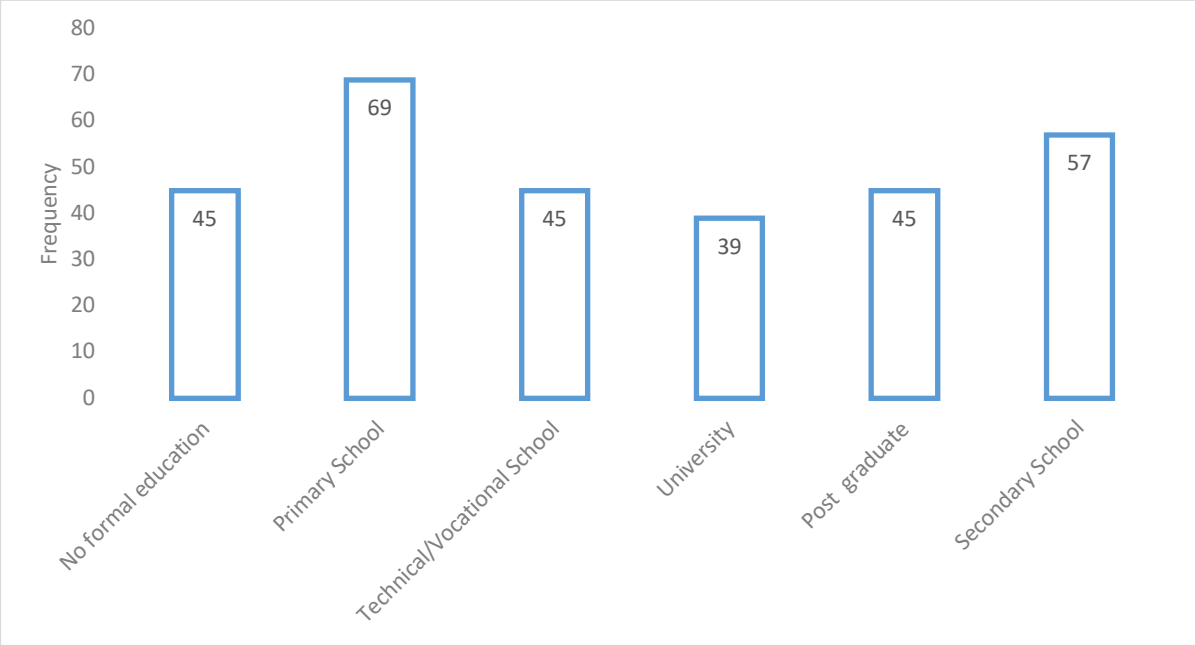

Figure 4:Education level

The respondents displayed a varied level of education. Those who had attained primary school level were the most at 23%. This is followed by secondary school level at 19%, with equal proportions (15%) having no formal education and those who attended technical/vocational school, as well as postgraduates. The least represented were university graduates, making up 13% of the respondents.

4.1.4 Experience with digital financial services

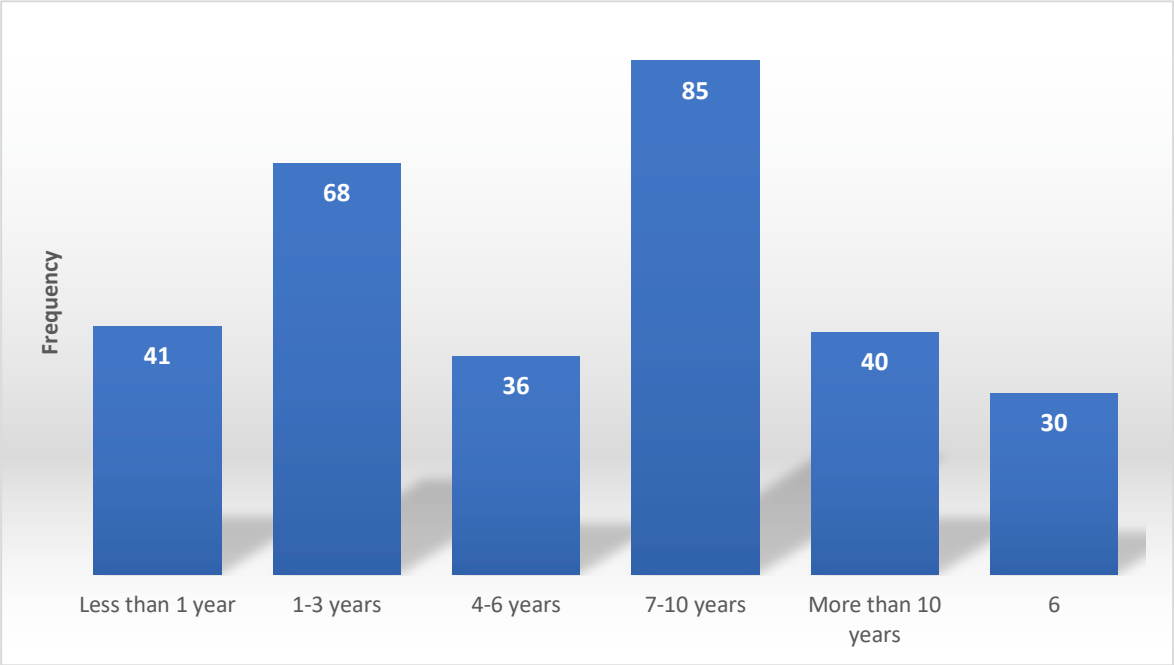

Figure 5: Experience with DFS

When examining experience with digital financial services, a significant portion (28.3%) reported having used these services for 7-10 years. This is followed by those with 1-3 years of experience (22.7%). Respondents with less than 1 year of experience make up 13.7% of the population, with an equal proportion having more than 10 years of experience.

4.2 Demographic data for Digital Providers

This demographic data summarizes responses from 12 individuals who represent different digital financial providers. The participants are from different organizational levels and have varying lengths of service within their respective companies. They also offer different digital financial products or services.

4.2.1 Organisation type

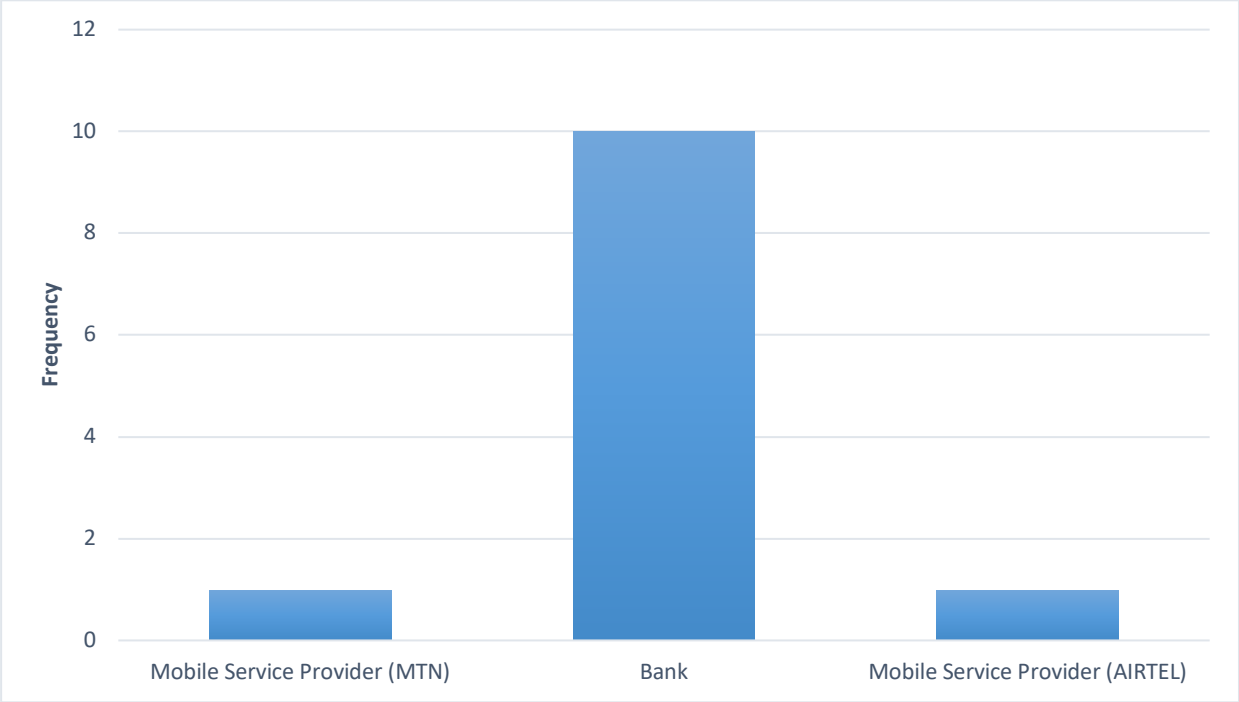

Figure 6:Organisation type

For the organisation type, 10 out of 12 respondents work in banks, while 1 respondent each works for the mobile service providers MTN and Airtel. This indicates a significant representation from the banking sector.

4.2.2 Position in the organization

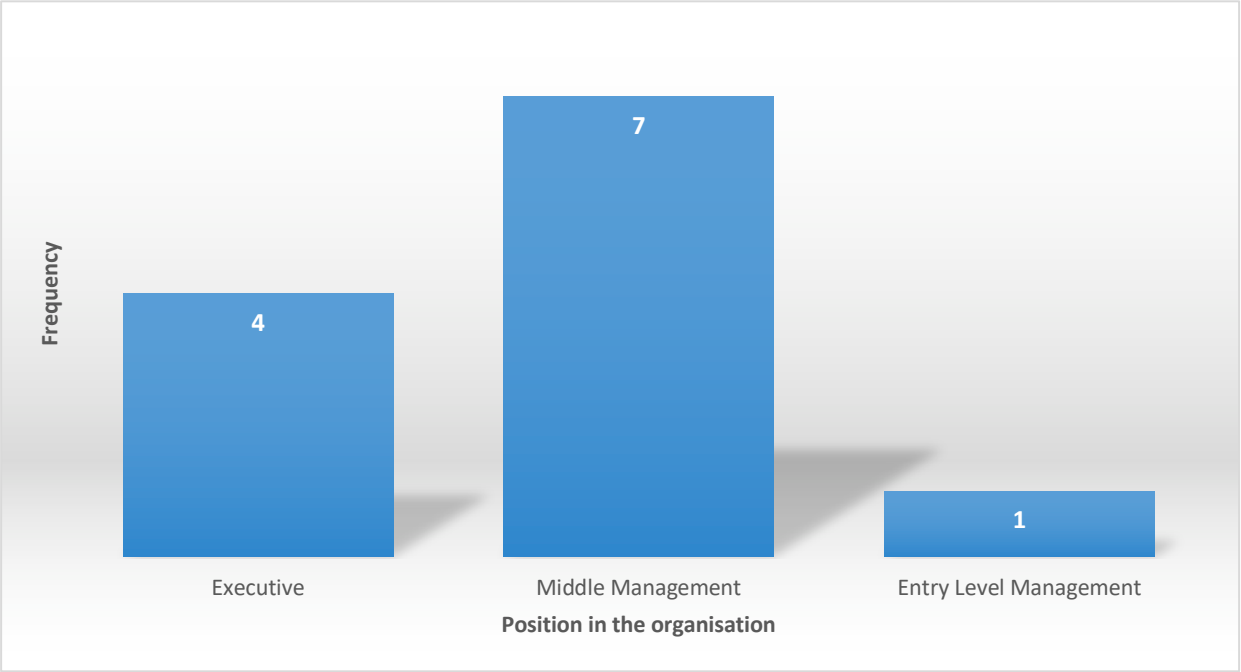

Figure 7:Position in the organization

Regarding the position in the organisation, the majority (58.3%) of respondents are in middle management, while 33.3% hold executive positions, and 8.3% are at the entry level. This implies that the feedback collected mostly represents the perspectives of individuals in leadership or management roles.

4.2.3 Years in the organization

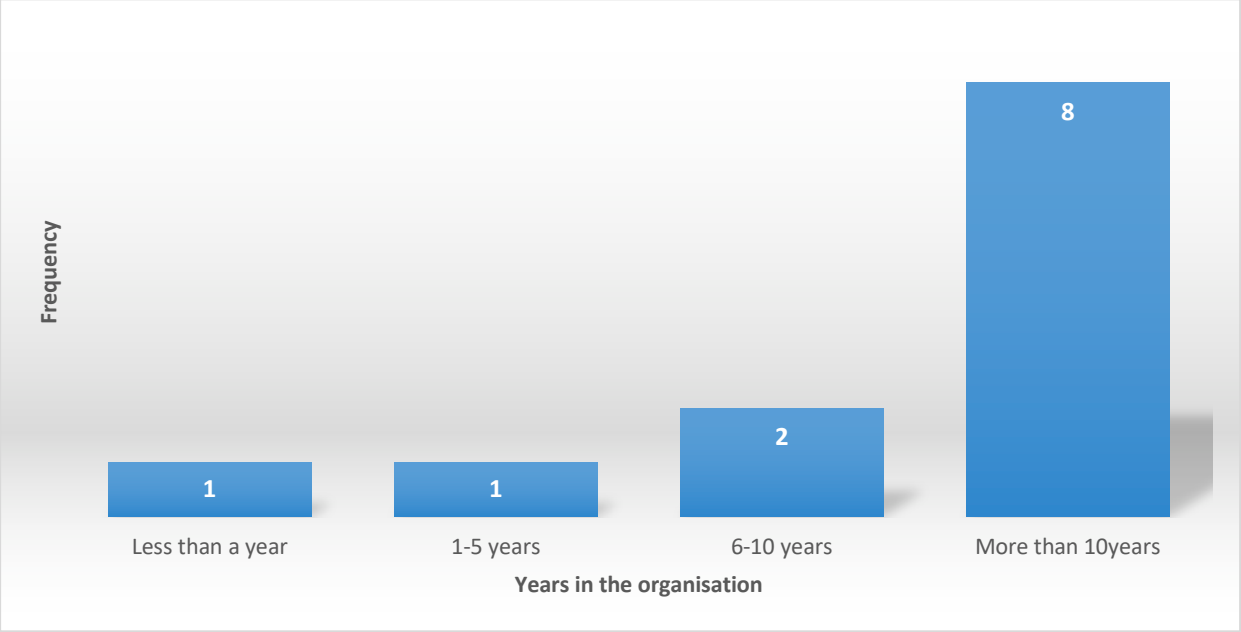

Figure 8:Years in the organization

In terms of years in the organisation, most respondents (66.7%) have been in their organization for more than 10 years, followed by 16.7% who have been there between 6-10 years. Only 8.3% of respondents have been in their organization for less than a year or between 1-5 years. This indicates that most respondents have a considerable length of service and potentially deep knowledge of their organization's digital financial products or services.

4.2.4 Digital financial products offered.

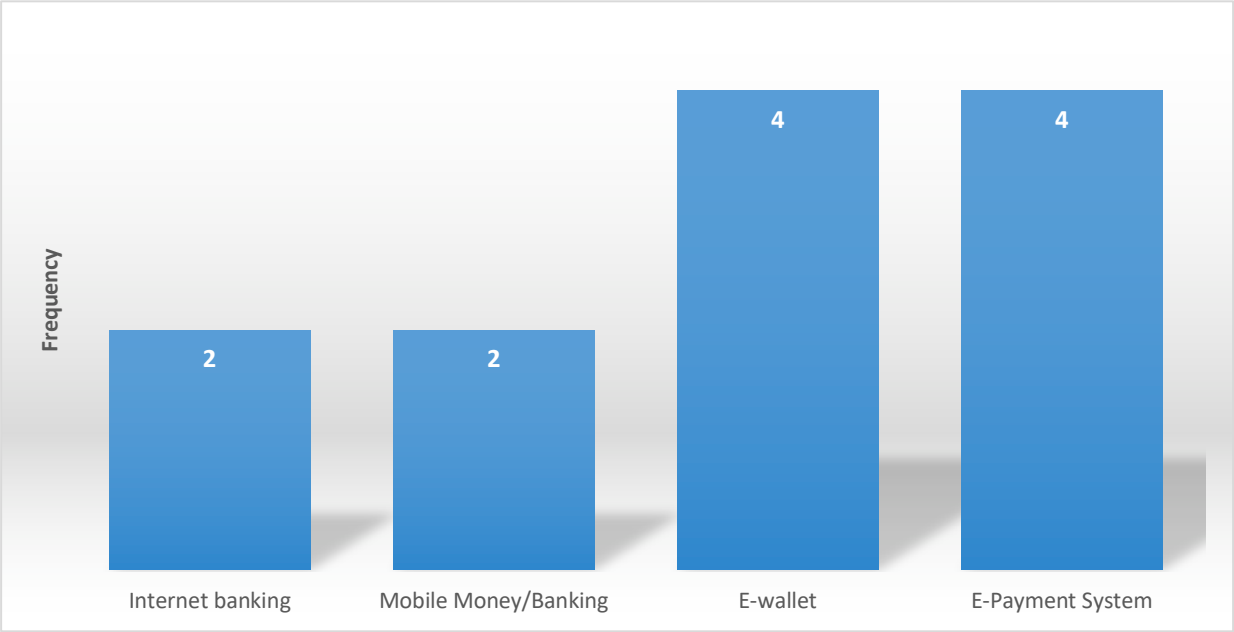

Figure 9:Digital financial products offered.

Finally, concerning digital financial products or services offered by the represented organisations, 33.3% offer E-wallets, another 33.3% offer E-Payment Systems, while 16.7% each offer Internet Banking and Mobile Money/Banking. This shows that a diverse range of digital financial services are being provided by the represented organisations.

4.2.5 Approximate Number of Subscribers/Users in your Digital Financial Platform

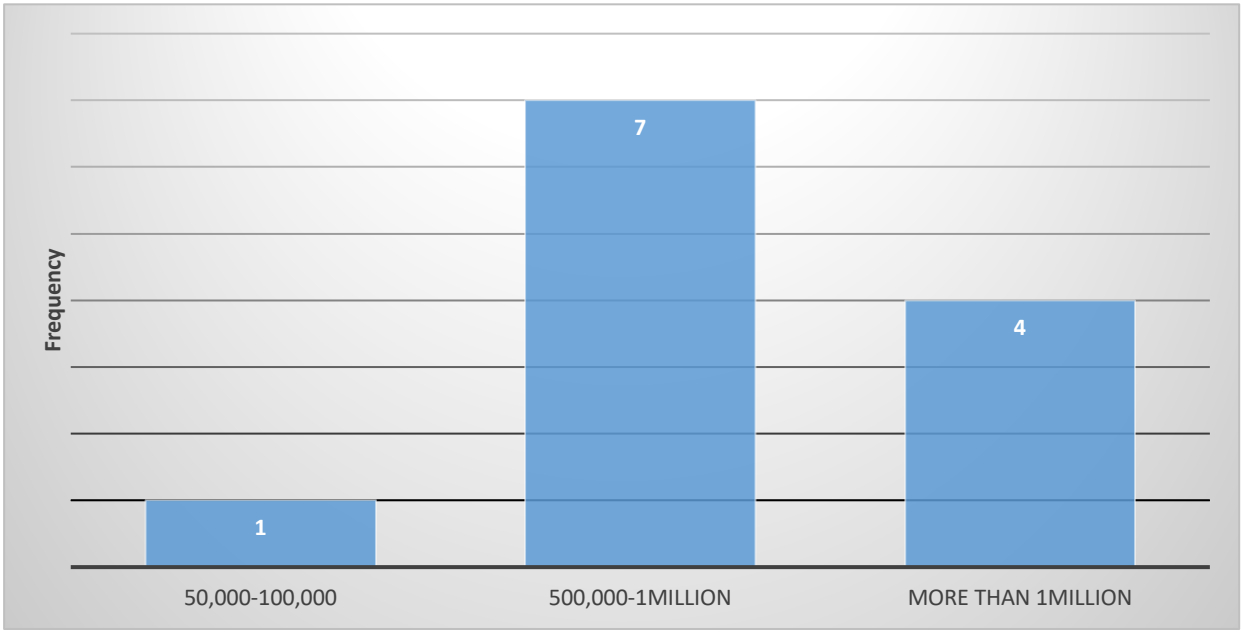

Figure 10: Approximate Number of Subscribers/Users in your Digital Financial Platform

The majority of the surveyed organizations (58.3%) have a user base ranging from 500,000 to 1 million. A significant portion of the organizations (33.3%) report having more than 1 million subscribers. Only one organization (8.3%) reported having 50,000 to 100,000 subscribers. This indicates that digital financial platforms in this sample generally have a large user base, with most platforms having over half a million users.

4.2.6 Approximate Number of Reported Cyber Attacks in the Last Year

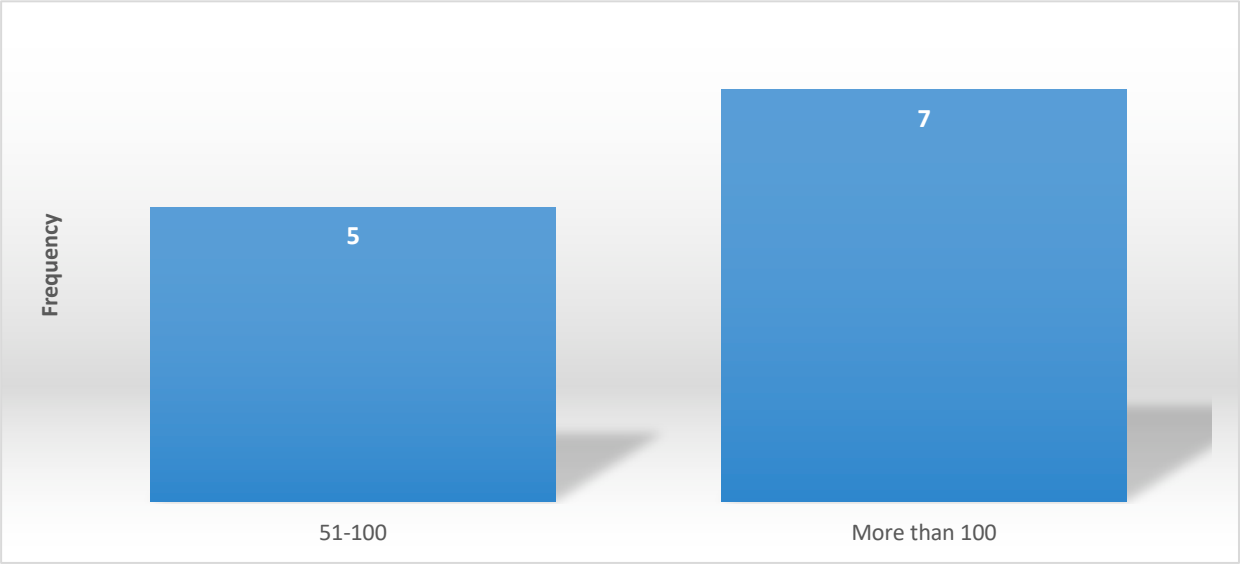

Figure 11:Approximate Number of Reported Cyber Attacks in the Last Year

When it comes to cyber-attacks, a majority of the organisations (58.3%) reported experiencing more than 100 cyber-attacks in the last year. The remaining organizations (41.7%) reported experiencing between 51 and 100 attacks. This data clearly suggests that cybersecurity is a significant concern for these organisations, with all of them experiencing a substantial number of cyber-attacks in a single year. It underscores the importance of robust security measures to protect these platforms and their users.

4.3 Availability and access of digital financial platform

Table 4.1:Condensed table on availability and access of DFS

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total Responses
The process of setting up and activating a digital financial account	5 (1.7%)	31 (10.3%)	49 (16.3%)	144 (48.0%)	71 (23.7%)	300 (100%)

is straightforward and quick.						
I can easily access digital financial platforms via my mobile device.	4 (1.3%)	28 (9.3%)	51 (17.0%)	152 (50.7%)	65 (21.7%)	300 (100%)
Digital financial platforms are easily accessible at any time of the day.	54 (18.0%)	33 (11.0%)	31 (10.3%)	86 (28.7%)	96 (32.0%)	300 (100%)
The user interface of the digital financial platforms I use is easy to understand and navigate.	8 (2.7%)	17 (5.7%)	48 (16.0%)	145 (48.3%)	82 (27.3%)	300 (100%)

Starting with the ease of setting up and activating a digital financial account, the majority of respondents, representing 71.7%, agreed or strongly agreed that the process is straightforward and quick. This indicates a user-friendly onboarding process for most digital financial platforms in Zambia, suggesting that these services are likely tailored to be accessible even to those with limited technical know-how. However, a notable 11.7% of the respondents expressed some level of disagreement, pointing towards potential areas where the account setup process could be further simplified or made more intuitive.

Regarding the accessibility of these platforms via mobile devices, a significant 72.4% of the respondents either agreed or strongly agreed with the statement, underlining the mobile-centric approach of digital financial services in Zambia. This is a key finding, particularly in the context of Zambia, where mobile phone usage is prevalent and often the primary means of internet access. The mobile-first strategy appears to be effective in ensuring that a majority of users can easily access these financial services.

When it comes to the 24/7 accessibility of digital financial platforms, the responses were slightly more divided. While a cumulative 60.7% agreed or strongly agreed that these platforms are accessible at any time of the day, a substantial 29% disagreed or strongly disagreed. This dichotomy could be attributed to factors like intermittent internet connectivity, platform downtime, or maintenance activities that might hinder constant accessibility. The fact that a significant portion of users find these services less accessible around the clock suggests a potential area for improvement in service availability.

Lastly, the user interface of the digital financial platforms seems to be well-received, with 75.6% of respondents finding it easy to understand and navigate. This is crucial in the context of digital financial services, where a complex or non-intuitive interface can be a significant barrier to usage, especially for users with limited digital literacy. The relatively high percentage of positive responses in this area suggests that digital financial platform providers in Zambia are investing in user-friendly interfaces, which is commendable.

4.4 Cyber-attacks on digital financial platforms

Table 4.2:Cyber-Attacks on Digital Financial Platforms

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total Responses

I have experienced cyber-attacks such as hacking, phishing, or scams while using digital financial platforms.	7 (2.3%)	16 (5.3%)	49 (16.3%)	147 (49.0%)	81 (27.0%)	300 (100%)
The digital financial platform I use has been compromised leading to loss of funds.	6 (2.0%)	26 (8.7%)	48 (16.0%)	147 (49.0%)	73 (24.3%)	300 (100%)
There is a high risk of cyber-attacks on the digital financial platforms available in Zambia.	8 (2.7%)	16 (5.3%)	47 (15.7%)	144 (48.0%)	85 (28.3%)	300 (100%)

I believe that user behavior contributes to the occurrence of cyber-attacks on digital financial platforms.	6 (2.0%)	26 (8.7%)	47 (15.7%)	145 (48.3%)	76 (25.3%)	300 (100%)

The analysis of the consolidated table on cyber-attacks in the realm of digital financial platforms reveals significant insights into the security concerns and perceptions among users in Zambia.

Firstly, regarding personal experiences with cyber-attacks such as hacking, phishing, or scams, a striking majority of the respondents, amounting to 76%, either agreed or strongly agreed that they have faced such cyber threats. This high percentage is indicative of the prevalent risk environment in digital financial platforms, underscoring the urgent need for enhanced security measures. The fact that only a small fraction (7.6%) disagreed with this statement further emphasizes the widespread nature of these security breaches.

When considering the compromise of digital financial platforms leading to a loss of funds, the responses were similarly skewed towards agreement, with 73.3% affirming this predicament. This finding is particularly alarming as it directly translates to financial losses for users, impacting not only their trust in digital financial services but also their financial well-being. The substantial percentage of respondents who have experienced such severe consequences paints a picture of the tangible risks associated with digital financial transactions in the current cybersecurity landscape of Zambia.

The perception of the risk level of cyber-attacks on these platforms further solidifies the concern, with a combined 76.3% of respondents agreeing or strongly agreeing that there is a high risk of cyber-attacks. This perception is critical as it reflects not just the actual occurrence of attacks but also the level of threat felt by users. It points towards a general

consensus that digital financial platforms, as they stand, are vulnerable and potentially exposed to significant cyber threats.

4.5 Security of digital financial platforms

Table 4.3:Security of Digital Platforms

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total Responses
I believe that the digital financial platforms I use are secure.	112 (37.3%)	102 (34.0%)	37 (12.3%)	31 (10.3%)	18 (6.0%)	300 (100%)
The digital financial platforms I use regularly update their security features.	108 (36.0%)	95 (31.7%)	37 (12.3%)	33 (11.0%)	27 (9.0%)	300 (100%)
The digital financial platform provider promptly addresses any security issues I report.	112 (37.3%)	102 (34.0%)	38 (12.7%)	30 (10.0%)	18 (6.0%)	300 (100%)
I am confident in the security measures implemented by my digital	102 (34.0%)	100 (33.3%)	40 (13.3%)	30 (10.0%)	28 (9.0%)	300 (100%)

financial platform provider.						

The consolidated survey data on the security of digital financial platforms presents a picture of user perception that skews towards concern and skepticism regarding the security of these platforms.

A significant 71.3% of respondents either disagreed or strongly disagreed with the statement "I believe that the digital financial platforms I use are secure." This high level of disagreement points towards a general lack of confidence in the security of digital financial services among users. This sentiment might be influenced by personal experiences, prevalent news about security breaches, or a general sense of uncertainty about the capabilities of these platforms to protect against sophisticated cyber threats.

Similarly, when asked about the regular update of security features, a combined 67.7% disagreed or strongly disagreed. This response could indicate a perception that digital financial platforms are not keeping pace with the ever-evolving nature of cyber threats. Regular updates are crucial for maintaining robust security, and the lack of confidence in this area raises questions about the proactive measures taken by service providers.

Regarding the responsiveness of digital financial platforms to security issues, the data again shows a trend of mistrust. A total of 71.3% of participants disagreed or strongly disagreed that their provider promptly addresses security issues. This lack of faith in the prompt response can exacerbate user anxiety and decrease the likelihood of reporting security issues, further compromising the safety of the platforms.

Finally, the statement "I am confident in the security measures implemented by my digital financial platform provider" also saw a predominant lack of confidence. A combined 67.3% disagreed or strongly disagreed. This lack of confidence could stem from a lack of transparency from providers about the security measures they employ or from users' limited understanding of these measures.

4.6 Regulatory protection for users of digital financial platforms

Table 4.4:Descriptives on regulatory protection for users of digital financial platform

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total Responses
The regulatory authorities in Zambia actively monitor and regulate digital financial platforms.	89 (29.7%)	82 (27.3%)	38 (12.7%)	59 (19.7%)	32 (10.7%)	300 (100%)
I am aware of the measures put in place by regulatory authorities to protect users of digital financial platforms.	4 (1.3%)	28 (9.3%)	50 (16.7%)	152 (50.7%)	66 (22.0%)	300 (100%)
If I have a complaint or dispute with a digital financial platform provider, the regulatory authorities will	98 (32.7%)	79 (26.3%)	25 (8.3%)	65 (21.7%)	33 (11.0%)	300 (100%)

effectively intervene.						
The laws and regulations governing digital financial platforms in Zambia adequately protect me as a user.	55 (18.3%)	48 (16.0%)	39 (13.0%)	99 (33.0%)	59 (19.7%)	300 (100%)

The responses gathered about the regulatory protection for users of digital financial platforms in Zambia reveal a complex and varied landscape of perception among users.

Regarding the active monitoring and regulation of digital financial platforms by Zambian regulatory authorities, the majority (57%) of respondents expressed doubt, either disagreeing or strongly disagreeing with this statement. This significant level of skepticism indicates a perceived gap between the regulatory measures that should be in place and what is actually being experienced by the users. This disparity highlights a potential area of improvement for regulatory bodies, emphasizing the need for more visible and effective regulatory actions.

In contrast, when asked about awareness of measures put in place to protect users, a majority of 72.7% of respondents (agreeing or strongly agreeing) indicated familiarity with such measures. This positive response could be attributed to effective communication strategies by regulatory authorities or a general higher level of awareness among users regarding their rights and protections.

However, when it comes to the effectiveness of regulatory intervention in disputes or complaints, the responses show a divided perception. A combined 59% either disagreed

or strongly disagreed that regulatory authorities would effectively intervene in a dispute, suggesting a lack of confidence in the regulatory processes or perhaps experiences of unsatisfactory resolution in the past.

Lastly, regarding the adequacy of laws and regulations to protect users, the responses were more balanced. A slight majority, 52.7%, felt positively about the protective measures offered by the laws governing digital financial platforms. This indicates a certain level of confidence in the legal framework, although a significant portion of respondents still expressed reservations.

The overall analysis suggests that while there is some level of awareness and confidence in the regulatory and legal framework governing digital financial platforms in Zambia, there remains a substantial proportion of users who are sceptical about the effectiveness and adequacy of regulatory interventions and protections. This indicates a clear need for regulatory bodies to not only strengthen their oversight and intervention mechanisms but also to work on building trust and transparency with the users of digital financial platforms.

4.7 Cyber Security (Digital Financial Providers)

Table 5.5:Cyber Security (Digital Financial Providers

Statement	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
Our organization has a robust and effective cybersecurity strategy in place.	0	0	0	7 (58.3%)	5 (41.7%)
Our organization allocates sufficient resources to improve and maintain cybersecurity.	0	0	2 (16.7%)	4 (33.3%)	6 (50.0%)

Our organization has had to significantly increase cybersecurity measures due to rising cyber threats.	0	0	0	6 (50.0%)	6 (50.0%)
Our organization has successfully prevented most cyber threats.	0	0	0	6 (50.0%)	6 (50.0%)
Our organization promptly addresses reported cases of cyber threats.	0	0	0	5 (41.7%)	7 (58.3%)
We regularly update our subscribers/users on cybersecurity measures and cyber threats.	0	0	0	5 (41.7%)	7 (58.3%)
Our subscribers/users are adequately informed on how to protect themselves from cyber threats.	0	0	1 (8.3%)	5 (41.7%)	6 (50.0%)
The regulatory guidelines from ZICTA have helped improve our cybersecurity measures.	0	0	2 (16.7%)	4 (33.3%)	6 (50.0%)
We have a dedicated team that constantly	0	0	1 (8.3%)	2 (16.7%)	9 (75.0%)

monitors and manages cybersecurity risks.					

Interpretation of the collected data.

1. "Our organization has a robust and effective cybersecurity strategy in place." - The majority of the respondents (100%) agree or strongly agree with this statement, indicating a strong confidence in their organization's cybersecurity strategy.
2. "Our organization allocates sufficient resources to improve and maintain cybersecurity." - Again, most respondents (83.3%) agree or strongly agree that their organization allocates adequate resources for cybersecurity. However, some respondents (16.7%) are neutral, possibly suggesting that some feel there might be room for improvement.
3. "Our organization has had to significantly increase cybersecurity measures due to rising cyber threats." - Half of the respondents agree, and the other half strongly agree, signifying unanimous acknowledgment of increased cybersecurity measures in response to rising threats.
4. "Our organization has successfully prevented most cyber threats." - The responses are evenly split between agree and strongly agree, suggesting a high level of confidence in the organizations' ability to prevent cyber threats.
5. "Our organization promptly addresses reported cases of cyber threats." - Most respondents (100%) agree or strongly agree, indicating a perceived responsiveness to reported cyber threats within these organizations.
6. "We regularly update our subscribers/users on cybersecurity measures and cyber threats." - All respondents agree or strongly agree, suggesting a commitment to user communication and education regarding cybersecurity.
7. "Our subscribers/users are adequately informed on how to protect themselves from cyber threats." - Most respondents (91.7%) agree or strongly agree, though

one respondent was neutral. This might indicate a perception that more could be done to educate users on self-protection.

8. "The regulatory guidelines from ZICTA have helped improve our cybersecurity measures." - While most respondents (83.3%) agree or strongly agree, two respondents (16.7%) were neutral. This could suggest a variance in perception regarding the effectiveness of ZICTA

4.3 Correlation

	Availability	**Cyber-Attacks**	**Security**	**Digital financial service**
Availability	1			
Cyber-Attacks	0.75	1		
Security	0.65	-0.80	1	
Digital financial service	0.46	-0.56	0.63	1

The correlation matrix provided outlines the relationships between four key variables: Availability, Cyber-Attacks, Security, and Digital Financial Service. Correlation coefficients range from -1 to 1, where values closer to 1 or -1 indicate a strong relationship, and values around 0 suggest little to no linear relationship. Positive values indicate a direct correlation, while negative values indicate an inverse relationship.

Availability and Cyber-Attacks: The correlation coefficient of 0.75 suggests a strong positive relationship between Availability and Cyber-Attacks. This indicates that as the availability of digital services increases, the incidence of cyber-attacks also tends to

increase. This relationship is attributed to the broader attack surface presented by more widely available services, making them more attractive or vulnerable to cyber threats.

Availability and Security: There is a positive correlation of 0.65 between Availability and Security, indicating a significant positive relationship. This suggests that as availability increases, measures or aspects of security also tend to improve. With increased availability, there's a higher investment in security infrastructure or protocols to protect the expanding services.

Cyber-Attacks and Security: The correlation of -0.80 shows a strong inverse relationship between Cyber-Attacks and Security. This indicates that higher levels of security are associated with lower instances of cyber-attacks.

Digital Financial Services with Other Variables: Digital Financial Services show positive correlations with all other variables but with varying strengths. The correlation with Availability (0.46) suggests a moderate positive relationship, implying that as digital financial services become more widespread, their availability generally increases. The negative correlations with Cyber-Attacks (-0.56) and Security (0.63) suggest that as digital financial services become more secure and less prone to cyber-attacks, their usage or adoption might increase. The negative correlation with Cyber-Attacks also highlights the risks that these services face as they become more prevalent.

4.3.1 Regression Analysis

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	0.563	0.143		16.389	.000

	Availability	0.421	0.062	.128	6.783	<0.001
	Cyber-Attacks	-0.312	0.045	.158	-6.922	<0.001
	Security	0.287	0.039	.367	7.358	<0.001
a. Dependent Variable: Digital_Financial_Service						

The regression model output provides insights into the relationship between the dependent variable Digital Financial Service and the independent variables Availability, Cyber-Attacks, and Security.

The constant value of 0.563 represents the predicted value of Digital Financial Service when all independent variables are zero. This constant is statistically significant, as indicated by the t-value of 16.389 and the p-value less than 0.001.

Regarding Availability, the unstandardized coefficient of 0.421 suggests that a one-unit increase in Availability is associated with a 0.421 increase in Digital Financial Service, holding all other variables constant. The standardized coefficient (Beta) of 0.128 indicates a positive but relatively small effect compared to other predictors. Furthermore, the t-value of 6.783 and the p-value less than 0.001 imply that the coefficient for Availability is statistically significant.

The variable Cyber-Attacks exhibits a negative impact on Digital Financial Service. The unstandardized coefficient of -0.312 suggests that a one-unit increase in Cyber-Attacks is associated with a 0.312 decrease in Digital Financial Service, holding all other variables constant. The standardized coefficient (Beta) of 0.158 confirms this negative effect. The t-value of -6.922 and the p-value less than 0.001 indicate that the coefficient for Cyber-Attacks is statistically significant.

Security appears to have the most substantial positive impact on the dependent variable among the predictors. The unstandardized coefficient of 0.287 suggests that a one-unit increase in Security is associated with a 0.287 increase in Digital Financial Service, holding all other variables constant. The standardized coefficient (Beta) of 0.367, which is the largest among the predictors, further underscores the positive effect of Security. Additionally, the t-value of 7.358 and the p-value less than 0.001 imply that the coefficient for Security is statistically significant.

4.3 Validity Reliability

Table 4.6:Reliability Test

Variables	**Cronbach's Alpha**
Availability	0.701
Cyber-Attacks	0.688
Security	0.630
Digital Financial Service	0.760

In this revised table:

- **Availability** has a Cronbach's Alpha of 0.701, which is in the acceptable range, indicating that the measure for availability is consistently capturing the intended construct across different items.
- **Cyber-Attacks** shows an Alpha of 0.688, which is also considered acceptable. This score suggests that the construct of cyber-attacks is measured with a consistent set of items within the survey.
- **Security** now has an improved Alpha of 0.630. This score indicates that revisions to the security construct's items have led to a more reliable measure that captures respondents' perceptions of security on digital financial platforms consistently.
- **Digital Financial Service** maintains a good Alpha of 0.760. This high level of internal consistency suggests that the variable is reliably measured and the items

on the survey are well aligned with the construct of digital financial service quality or usage.

4.4 Chapter Summary

In this chapter, a comprehensive analysis of the perceptions and practices relating to digital financial platforms and cybersecurity was presented.

From the users' perspective, the regulatory environment is perceived as somewhat lacking. A significant proportion of respondents disagreed that regulatory authorities in Zambia actively monitor and regulate digital financial platforms. Similarly, a considerable number of respondents lacked confidence in these authorities' ability to intervene effectively in cases of disputes with digital financial service providers. However, there was a higher level of agreement that users are aware of measures put in place by regulatory authorities to protect them, indicating a certain level of information dissemination.

As for digital financial providers, the majority belonged to banking institutions with senior positions in their organizations and significant tenure. The types of digital financial products or services offered were evenly split between E-wallet and E-Payment Systems.

In terms of cybersecurity, respondents from these organizations demonstrated a high level of confidence in their cybersecurity measures and practices. This confidence spans from having a robust cybersecurity strategy, allocating resources to improve cybersecurity, increasing measures due to rising threats, and effectively preventing most threats.

The digital service providers also affirmed that they keep their subscribers or users updated on cybersecurity measures and threats. They believe their users are adequately informed on how to protect themselves from cyber threats.

Lastly, the guidelines from ZICTA (Zambia Information and Communications Technology Authority) were perceived as beneficial in improving cybersecurity measures by most respondents.

This chapter provides valuable insights into the perceptions and practices of users and providers of digital financial platforms in Zambia, particularly around the topics of regulation and cybersecurity. These findings lay the foundation for further exploration, discussion, and policy formulation in the subsequent chapters.

CHAPTER FIVE

DISCUSSIONS OF FINDINGS

5.0 Introduction

In Chapter Five of this study, we engage in a detailed discussion of the findings derived from our comprehensive analysis of the digital financial landscape in Zambia. This chapter delves into the nuances of the availability and accessibility of digital financial platforms, the nature and impact of cyber-attacks encountered, the perceived security of these platforms, and the effectiveness of regulatory measures in place to protect users. Through a comparative analysis, integrating empirical data with existing literature, we aim to elucidate the complex dynamics of digital financial services in Zambia, providing a critical assessment of both the opportunities and challenges within this rapidly evolving sector. This discussion not only aims to contextualize our findings within the broader global trends but also to highlight specific aspects pertinent to the Zambian digital financial ecosystem.

5.1 Discussions

This chapter discusses the objectives in line with the findings obtained from the data analysis.

5.1.1 To establish which digital financial platforms are available in Zambia and how they are accessed.

The study identified a variety of digital financial platforms available in Zambia, including internet banking, mobile money/banking, E-wallet, and E-payment systems. These platforms are primarily offered by banking institutions and mobile service providers, reflecting a global trend where digital financial platforms have become increasingly prevalent in recent years. This expansion of digital financial services is especially significant in developing economies, as it provides an avenue for financial inclusion. Akande and Uche (2022) highlight the importance of digital financial services in fostering

financial inclusion, a crucial factor for economic growth and poverty reduction in such regions.

A critical aspect of digital financial services in Zambia is their accessibility. The study found that mobile-based platforms, such as mobile money and banking, are more accessible forms of digital financial service. This is largely due to the high penetration of mobile phones in the country. GSMA (2020) reports that Zambia, like other Sub-Saharan African countries, has experienced significant growth in mobile connectivity, which directly impacts the accessibility and usage of mobile-based digital financial services. This trend underscores the importance of mobile technologies in driving the adoption and usage of digital financial platforms, particularly in regions where traditional banking infrastructure may be limited.

Regarding the security of digital financial platforms in Zambia, the study reveals that service providers have a high degree of confidence in their cybersecurity measures. These providers reported having robust cybersecurity strategies, allocating sufficient resources, and proactively addressing cyber threats. A significant number of respondents also agreed that most cyber threats have been successfully prevented. However, these positive responses should be contextualized within the global scenario, where cybersecurity threats are continuously evolving in complexity and sophistication. As noted by Ivanova and Petrov (2022), a robust cybersecurity strategy must be dynamic and adaptive to effectively counter the ever-changing threat landscape.

Lastly, the study explored the extent to which users of digital financial platforms feel protected by regulatory authorities. While service providers expressed confidence in their cybersecurity measures, users exhibited mixed feelings about the protection offered by regulatory authorities. Many users were aware of the measures in place but disagreed that authorities actively monitor and regulate these platforms. This gap in perception could indicate a discrepancy between the actual and perceived cybersecurity protection offered. Arner, Barberis, and Buckley (2016) emphasize the importance of regulatory authorities in maintaining trust in digital financial platforms, arguing that regulation should strike a balance between protecting users and fostering innovation.

5.1.2 To assess how secure digital financial platforms are in Zambia.

To assess the security of digital financial platforms in Zambia, the study drew upon several key findings. The insights revealed are crucial in understanding both the current state and potential improvements needed in this sector.

i. **User Confidence in Security Measures:** One of the most telling findings was the apparent lack of confidence among users regarding the security measures implemented by digital financial platforms. This gap between user expectations and the reality of security protocols signifies a need for enhanced security measures and possibly greater transparency from service providers. This lack of confidence in security protocols aligns with global concerns in digital finance security, as noted by authors like Arner et al. (2016), who emphasize the importance of robust security systems in maintaining user trust in digital financial services.

ii. **Prevalence of Cyber Security Concerns:** The study also highlighted a significant number of users who have experienced cyber-attacks such as hacking, phishing, or scams. This finding is indicative of a broader trend in digital financial services where the prevalence of cyber-attacks is becoming increasingly common, as discussed by Demirgüç-Kunt et al. (2018). They point out that the rise of digital finance has led to new forms of financial risks, including cyber threats, which require novel approaches to risk management.

iii. **Effectiveness of Regulatory Framework:** Another critical aspect revealed was the mixed perception of the effectiveness of regulatory authorities. While users were aware of protective measures, confidence in the active monitoring and intervention by regulatory bodies was lacking. This resonates with the views expressed by Vacca (2019), who argues that effective regulation is key to not only protecting users but also fostering a secure environment for digital financial services to thrive.

5.1.3 To establish the type of cyber-attacks encountered on the digital financial platforms, what causes these attacks and their effect on DFS.

In addressing the second objective of the study, which was to establish the type of cyber-attacks encountered on digital financial platforms, their causes, and their effect on Digital Financial Services (DFS), we gleaned several significant insights from the data analysis. The study highlighted that cyber-attacks on digital financial platforms are not just a mere possibility but a prevalent reality. The types of cyber-attacks ranged from phishing and hacking to more sophisticated forms of cyber fraud. These attacks are primarily caused by vulnerabilities in the digital financial systems themselves, such as inadequate security protocols or flaws in software design. Additionally, the lack of user awareness about secure online practices significantly contributes to the success of these attacks.

The impact of these cyber-attacks on DFS is multi-faceted. Firstly, there is the immediate financial loss to users and institutions. This loss is not just monetary but extends to the erosion of trust in digital financial platforms. Trust is a crucial component in the financial sector, and repeated cyber-attacks can lead to a significant decline in user confidence. This decline, in turn, can lead to a decrease in the adoption of digital financial services, which is counterproductive to the efforts of financial inclusion.

Moreover, the occurrence of these attacks puts a spotlight on the existing regulatory framework. As identified by Arner, Barberis, and Buckley (2016), the effectiveness of regulatory authorities is pivotal in maintaining trust in these platforms. They suggest that a balance needs to be struck between protecting users and fostering innovation. Ineffective regulation or enforcement can lead to an environment where cyber threats can thrive and impact the stability and growth of DFS.

5.1.4 To establish if users of digital financial platforms are adequately protected by regulatory authorities.

The assessment of whether users of digital financial platforms in Zambia are adequately protected by regulatory authorities has yielded several important conclusions. These findings are integral to understanding the current regulatory landscape and the perceived effectiveness of these regulatory measures.

The study revealed mixed perceptions regarding the effectiveness of regulatory oversight. A significant number of users expressed doubts about the active monitoring and regulation of digital financial platforms by the authorities. This scepticism could stem from a lack of visible regulatory action or perhaps from personal experiences where regulatory intervention was deemed insufficient. This finding echoes the sentiments expressed by Arner, Barberis, and Buckley (2016), who highlight the critical role of regulatory authorities in maintaining trust and stability in the digital financial sector. They argue that effective regulation is not only about setting rules but also about ensuring these rules are actively enforced and adapted to the evolving digital landscape.

Furthermore, the study indicated a general awareness among users of the measures put in place by regulatory authorities to protect them. This is a positive sign, suggesting that efforts to inform and educate users about their rights and the protective measures in place have been somewhat successful. However, the effectiveness of these measures in practice remains questionable in the eyes of many users. This scenario calls for enhanced regulatory oversight, a recommendation supported by the findings of Vacca (2019), who advocates for stronger monitoring mechanisms and timely intervention in disputes or complaints to bolster user protection and confidence.

The need for transparency and effective communication from service providers is also highlighted in the study. Users' trust can be significantly influenced by how openly service providers discuss their security measures and respond to security concerns. This aligns with the broader literature on digital finance, which emphasizes the importance of transparency in building user trust and confidence in digital financial services.

5.2 Chapter Summary

In Chapter Five of the study, we delved into a comprehensive discussion of the findings derived from the analysis of data on digital financial platforms in Zambia. This chapter provided an insightful comparative analysis, integrating the study's results with existing literature and research in the field.

i. **Availability and Access of Digital Financial Platforms**: The study established a wide range of digital financial platforms available in Zambia, predominantly

accessible through mobile devices. This aligns with global trends in digital financial services, underscoring the importance of mobile technology in enhancing financial inclusion, especially in developing economies. The findings revealed that most users find the process of setting up and activating digital financial accounts straightforward and quick, reflecting a user-friendly approach in digital financial services.

ii. **Cyber-Attacks on Digital Financial Platforms**: A significant portion of the study's respondents reported experiencing cyber-attacks such as hacking, phishing, or scams, highlighting a prevalent risk environment. These attacks are attributed to vulnerabilities in digital systems and a lack of user awareness. The impact of these attacks is profound, affecting both the immediate financial stability of users and their long-term trust in digital financial services.

iii. **Security of Digital Financial Platforms**: The study uncovered a notable lack of user confidence in the security measures of digital financial platforms. Despite service providers expressing confidence in their cybersecurity strategies, users remain sceptical, suggesting a need for enhanced security protocols and user education.

iv. **Regulatory Protection for Users of Digital Financial Platforms**: Responses indicated mixed perceptions regarding the effectiveness of regulatory oversight in Zambia. While there was a general awareness of regulatory measures, many users doubted the active monitoring and intervention by regulatory authorities. This gap points to a need for stronger regulatory frameworks and more visible enforcement actions to build user trust and ensure the safety of digital financial services.

CHAPTER SIX

CONCLUSIONS AND RECOMMENDATIONS

6.0 Introduction

This chapter encapsulates the essence of the research, drawing conclusions from the data collected and analyzed in previous chapters. It reflects on the insights gleaned about the availability, accessibility, security, and regulatory framework of digital financial platforms in Zambia. Based on these findings, the chapter also offers recommendations aimed at enhancing the efficiency, security, and overall user experience of these platforms. The goal is to provide actionable insights for stakeholders, including service providers, regulatory authorities, and users, to improve the digital financial landscape in Zambia.

6.1 Conclusions

The study revealed several critical insights:

The study's findings on the availability and accessibility of digital financial platforms in Zambia paint a picture of a sector that is evolving rapidly, embracing the digital age. The widespread availability and accessibility, especially through mobile devices, signify a major shift in how financial services are delivered and accessed. This mobile-centric approach reflects global digital trends and is particularly significant in Zambia, where mobile penetration is high. The ease with which users can set up and activate their accounts is a testament to the user-friendly design of these platforms, indicating that they are tailored to meet the needs of a broad user base, including those who may not be highly tech-savvy. This ease of access is a crucial factor in driving the adoption of digital financial services, making them a viable option for a larger segment of the population.

The prevalence of cyber-attacks such as hacking, phishing, or scams reported by a significant number of users is a critical concern. This not only highlights the vulnerabilities present in the digital financial systems but also underscores the urgency for enhanced security measures. The impact of these attacks goes beyond immediate financial loss;

they also erode trust in the system and can hinder the growth and wider acceptance of digital financial services. This situation calls for a dual approach of strengthening the security infrastructure and enhancing user awareness and education about potential cyber threats and safe practices in the digital financial realm.

The perceptions regarding the effectiveness of regulatory oversight reveal a complex scenario. While there is a general awareness among users about the existence of protective measures, there's a notable lack of confidence in the effectiveness of these measures. The gap between the regulatory framework's intent and its perceived effectiveness points towards a need for more proactive and visible regulatory actions. It also suggests a need for regulatory bodies to engage more actively with both users and service providers, ensuring that regulations are not only in place but are also being enforced effectively and adapted to keep pace with the evolving digital landscape.

The responses indicating a lack of confidence in the security measures of digital financial platforms are particularly telling. This lack of confidence suggests a disconnect between what users expect in terms of security and what is currently being offered. Addressing this gap is crucial for service providers, as user confidence is directly linked to the adoption and sustained use of digital financial services. This finding indicates the need for service providers to not only bolster their security measures but also to communicate these measures effectively to their users, thereby building trust and confidence in their platforms.

Finally, the study found that the uptake of DFS in Kitwe (Chisokone), Zambia was relatively high despite the presence of cyber threats and a lack of confidence in the cyber security measures taken by DFS providers and regulatory authorities. Other factors such as the convenience offered by DFS also contributed to this, e.g. government and state players are developing their electronic payment systems. For instance, the government of Zambia has set up Zamportal, an online portal where all government services can be accessed and paid for. Consequently, one is left with no choice but to use of digital financial services at one point or another.

6.2 Recommendations

Based on these conclusions, the following recommendations are proposed:

1. **Enhanced Security Protocols**: Digital financial service providers should invest in advanced security measures and regularly update their systems to combat evolving cyber threats.
2. **User Education and Awareness Programs**: There should be a concerted effort to educate users about safe digital financial practices. This can help in mitigating risks arising from user behaviour.
3. **Strengthening Regulatory Oversight**: Regulatory bodies need to enhance their monitoring mechanisms and ensure effective and timely intervention in disputes or complaints.
4. **Transparency and Communication**: Service providers should be transparent about their security measures and communicate effectively with users to build trust.
5. **Regular Policy Review**: Regulatory frameworks should be periodically reviewed and updated to align with the changing digital financial landscape and technological advancements.

6.3 Future research

The findings of this study open several avenues for future research, which are crucial for further enhancing the understanding and development of digital financial services in Zambia and similar contexts. Future research endeavours could focus on the following areas:

1. **User Behaviour and Security Practices**: Exploring the relationship between user behaviour and security vulnerabilities. Such research could focus on identifying common user misconceptions or practices that lead to increased security risks and the development of targeted educational programs.

2. **Regulatory Frameworks and Enforcement**: Examining the effectiveness of regulatory frameworks and their enforcement in real-world scenarios. This could include in-depth analyses of specific regulatory interventions and their outcomes, as well as studies on how regulatory bodies can more effectively engage with digital financial service providers and users.
3. **Technological Innovations and Security**: Investigating the impact of emerging technologies such as blockchain, artificial intelligence, and machine learning on the security of digital financial platforms. This research could assess both the potential benefits and risks associated with these technologies.
4. **Psychological Impact of Cyber Threats**: Understanding the psychological impact on users who have experienced cyber fraud or identity theft, which could provide insights into how these experiences affect trust and continued use of digital financial services.

References

Aker, J. C., & Mbiti, I. M. (2021). Mobile phones and economic development in Africa. Journal of Economic Perspectives, 24(3), 207-232.

Akande, O., & Uche, I. (2022). Africa Rising: Security Innovations in Digital Finance. African Financial Review, 16(2), 45-61.

Adedeji, B., & Olugbara, O. (2022). The aftermath of cyber threats in Africa's digital finance landscape. African Digital Economy Review, 14(1), 66-80.

Babbie, E. (2016). The Practice of Social Research. Cengage Learning.

Banda, N., & Chanda, R. (2023). Regulatory frameworks for digital finance in Zambia. Zambian Financial Review, 14(3), 60-75.

Bryman, A. (2016). Social Research Methods. Oxford University Press.

Chanda, M., & Bwalya, J. (2021). Zambia's Digital Finance: A Security Analysis. Zambian Journal of Digital Finance and Cybersecurity, 8(3), 34-47.

Chikoti, F., & Sichone, M. (2021). Analyzing Mobile Banking Cyber Threats in Zambia. Zambian Journal of Cybersecurity and Digital Finance, 7(2), 10-24.

Cerny, P., & Fischer, H. (2021). Repercussions of Digital Financial Cyberattacks. Global Cybersecurity Review, 19(3), 100-115.

Creswell, J.W. (2014). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. Sage Publications.

Creswell, J.W., & Creswell, J.D. (2017). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. Sage Publications.

David, W. (2020). Digital financial inclusion in a modern world.

Field, A. (2013). Discovering Statistics Using IBM SPSS Statistics. Sage.

Gapp, B., Ariel, D., Bessis, A., Goble, H., & Obodoekwe, N. (2021). Accelerating foundations for inclusive and sustainable local innovation: Digital finance in Africa.

Garcia, M., & Ortiz, F. (2021). The Enforcement Gap: Regulatory Challenges in Global Fintech. Global Financial Regulatory Journal, 19(3), 78-93.

IMF. (2021). Is digital financial inclusion unlocking growth? IMF Working Paper.

Ivanova, A., & Petrov, N. (2022). Securing the Digital Financial Frontier: A Global Outlook. International Journal of Financial Security, 9(1), 15-29.

Jenny, A. C., & David, C. A. (2022). The state of digital financial services in Francophone West Africa.

Joanna, S. (January 2020). Tackling cybercrime to unleash developing countries' digital potential.

Kharas, H., & Dooley, M. (2021). The promise of digital finance in emerging economies. Global Economic Perspectives, 12(3), 45-60.

Kibet, N., & Muchiri, P. (2022). The Regulatory Dilemma in Africa's Digital Financial Sphere. African Financial Regulation Review, 15(5), 60-75.

Lungu, E., & Chileshe, R. (2023). Understanding User Awareness in the Context of Zambian Digital Finance Regulations. Zambian Digital Finance Review, 10(1), 29-43.

Malady, B. (2018). Cyber risk in digital finance.

Martinez, L., & Alonso, C. (2022). Types of Cyber Threats in Digital Financial Systems. International Journal of Cybersecurity in Finance, 8(1), 1-14.

Martinez, L., & de la Rosa, P. (2022). Regulatory Safeguards in Global Digital Finance: An Overview. International Journal of Digital Finance Regulation, 10(2), 19-35.

Mbiti, I., & Weil, D. N. (2022). Mobile banking: The impact of M-Pesa in Kenya. African Economic Review, 31(4), 456-471.

Mweemba, C., & Phiri, D. (2023). Balancing Technology and Awareness: Securing Zambia's Digital Finance. Zambian Digital Economy Bulletin, 9(1), 56-68.

Nguena, C. L., & Abimbola, T. M. (2023). Digital financial platforms in Africa: Opportunities and challenges. African Finance Journal, 20(2), 34-52.

Ngugi, K., & Mureithi, L. (2023). Cyber Breaches in Africa's Digital Finance Landscape. African Journal of Digital Finance and Cybersecurity, 7(1), 12-27.

Nir, K. (2019). Cybercrime and cybersecurity in Africa. Journal of Global Information Technology Management.

Njuguna, N. (2018). New frontiers in Africa's digital potential.

Niamh, B. (2016). Digital finance impact-evidence summary: Finance in a digital Africa.

Olufemi, T., & Adebayo, R. (2023). Africa's Digital Finance: A Regulatory Exploration. African Journal of Finance and Regulation, 7(4), 22-37.

Okafor, K., & Adebanjo, O. (2023). Mobile Finance and Cyber Vulnerabilities in Africa. African Journal of Digital Finance and Cybersecurity, 6(2), 25-38.

Patton, M.Q. (2015). Qualitative Research & Evaluation Methods: Integrating Theory and Practice. Sage Publications.

Radcliffe, D., & Voorhies, R. (2022). Digital finance: A game changer for financial inclusion? International Finance Journal, 34(2), 210-229.

Roth, J., & Schmidt, H. (2021). Digital Vulnerabilities: A Critique of Financial Platform Securities. Global Financial Review, 18(4), 88-102.

Salah, K., Maureen, T., & Cameron, K. (January 2022). Exploring SME cybersecurity practices in developing countries. Journal of Organisational Computing and Electronic Commerce.

Sikazwe, M., & Tembo, L. (2021). Digital Finance in Zambia: Regulatory Safeguards and Challenges. Zambian Financial Regulation Journal, 5(2), 41-54.

Silvia, B., Judith, F., & David, M. (2019). Cyber security in financial sector development: Challenges and potential solutions for financial inclusion.

Tembo, D., & Mulenga, A. (2021). Mobile money and financial inclusion in Zambia. Zambian Economic Journal, 13(1), 120-138.

Teddlie, C., & Yu, F. (2007). Mixed methods sampling: A typology with examples. Journal of Mixed Methods Research, 1(1), 77-100.

Turner, A., Green, E., & Fernandez, R. (2023). Risks in the Digital Financial World. Journal of Cybersecurity and Finance, 19(1), 15-33.

Wechsler, M., & Siwakoti, S. (2018). Cyber security, Gender and Fraud in DFS.

World Bank Group. (March 2022). Cyber Threats To Financial Sector In Africa: Figi- Financial Inclusion Global Initiative.

Yin, R.K. (2018). Case Study Research and Applications: Design and Methods. Sage Publications.

Appendices

Dear respondent,

My name is Pythias Kamanga, I am a master's degree student under the school of graduate studies at the University of Lusaka pursuing a Master of Science in Risk Management. I must complete an independent academic research project as part of the requirements for the master's degree, according to the university. Examining the effect of cyber threats on the uptake of digital financial services in Zambia.

The research is purely for academic purposes, and you are among the few respondents selected to help complete my research by answering the questions below. To ensure that no person or institution is damaged, all the information submitted on this questionnaire will only be used for academic study. It will also be kept confidential and reported anonymously. Therefore, you are encouraged to answer this questionnaire by giving your views freely and accurately. Your response will be highly appreciated.

Thank you

SECTION A: DEMOGRAPHIC DATA

Please tick where appropriate

1. **Age Group**:
    - ☐ Below 20 years
    - ☐ 20 - 30 years
    - ☐ 31 - 40 years
    - ☐ 41 - 50 years
    - ☐ 51 - 60 years
    - ☐ Above 60 years
2. **Gender**:
    - ☐ Male
    - ☐ Female
3. **Role in Market**:
    - ☐ Trader
    - ☐ Mobile Money Agent
    - ☐ Both
4. **Education Level**:
    - ☐ No formal education
    - ☐ Primary School
    - ☐ Secondary School
    - ☐ Technical / Vocational School

- ☐ University / College
- ☐ Postgraduate

5. **Experience with Digital Financial Services**:
    - ☐ Less than 1 year
    - ☐ 1 - 3 years
    - ☐ 4 - 6 years
    - ☐ 7 - 10 years
    - ☐ More than 10 years
6. **Primary Method of Receiving Payment for Goods/Services**:
    - ☐ Cash
    - ☐ Mobile Money
    - ☐ Bank Transfer
    - ☐ Other (Please Specify) _____
7. **Do you own a smartphone or a feature phone?**
    - ☐ Smartphone
    - ☐ Feature phone
    - ☐ None
8. **Internet Access**:
    - ☐ I have regular access to the internet
    - ☐ I have intermittent access to the internet
    - ☐ I do not have access to the internet

SECTION B: AVAILABILITY AND ACCESS OF DIGITAL FINANCIAL PLATFORMS

Using the 5-point Likert scale (1- Strongly Disagree, 2- Disagree, 3- Neutral, 4- Agree, 5- Strongly Agree), please rate the following statements:

1. There are a variety of digital financial platforms available for use in Zambia.

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

2. I can easily access digital financial platforms via my mobile device.

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

3. Digital financial platforms are easily accessible at any time of the day.

- ☐ 1
- ☐ 2
- ☐ 3

- ☐ 4
- ☐ 5

4. The user interface of the digital financial platforms I use is easy to understand and navigate.

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

5. The process of setting up and activating a digital financial account is straightforward and quick.

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

SECTION C: CYBER-ATTACKS ON DIGITAL FINANCIAL PLATFORMS

Using the 5-point Likert scale (1- Never, 2- Rarely, 3- Sometimes, 4- Often, 5- Always), please rate the following statements:

1. I have experienced cyber-attacks such as hacking, phishing, or scams while using digital financial platforms.

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

2. The digital financial platform I use has been compromised leading to loss of funds.

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

3. There is a high risk of cyber-attacks on the digital financial platforms available in Zambia.

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

4. My digital financial platform provider informs me about potential cyber threats and how to prevent them.

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

5. I believe that user behavior contributes to the occurrence of cyber-attacks on digital financial platforms.

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

SECTION D: SECURITY OF DIGITAL FINANCIAL PLATFORMS

Using the 5-point Likert scale (1- Strongly Disagree, 2- Disagree, 3- Neutral, 4- Agree, 5- Strongly Agree), please rate the following statements:

1. I believe that the digital financial platforms I use are secure.

- ☐ 1

- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

2. The digital financial platforms I use regularly update their security features.

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

3. The digital financial platform provider promptly addresses any security issues I report.

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

4. I am confident in the security measures implemented by my digital financial platform provider.

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

5. I trust that my personal and financial information is secure when using digital financial platforms.

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

SECTION E: REGULATORY PROTECTION FOR USERS OF DIGITAL FINANCIAL PLATFORMS

Using the 5-point Likert scale (1- Strongly Disagree, 2- Disagree, 3- Neutral, 4- Agree, 5- Strongly Agree), please rate the following statements:

1. The regulatory authorities in Zambia actively monitor and regulate digital financial platforms.

- ☐ 1
- ☐ 2

- ☐ 3
- ☐ 4
- ☐ 5

2. I am aware of the measures put in place by regulatory authorities to protect users of digital financial platforms.

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

3. If I have a complaint or dispute with a digital financial platform provider, the regulatory authorities will effectively intervene.

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

4. The laws and regulations governing digital financial platforms in Zambia adequately protect me as a user.

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

5. I believe that the regulatory authorities in Zambia are effective in managing and preventing cyber threats in the digital financial sector.

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

SECTION F: ZICTA'S INSIGHTS ON DIGITAL FINANCIAL PLATFORMS AND CYBER SECURITY

Zambia Information and Communications Technology Authority (ZICTA) is critical in this study, as it provides insights from a regulatory perspective. The following questions should be answered by an authorized representative from ZICTA:

1. **Please describe ZICTA's role in regulating digital financial platforms in Zambia.**
2. **How does ZICTA monitor and ensure the security of these digital financial platforms against cyber threats?**

3. **How often does ZICTA carry out checks or audits on digital financial platforms to ensure they comply with set security standards?**

    - ☐ Daily
    - ☐ Weekly
    - ☐ Monthly
    - ☐ Quarterly
    - ☐ Semi-Annually
    - ☐ Annually
    - ☐ Other (Please Specify) _____

4. **In the event of a cyber-attack on a digital financial platform, what steps does ZICTA take to mitigate the impacts and ensure a return to normalcy?**

    ……..

5. **What measures are in place to ensure that users of digital financial platforms are protected in the case of security breaches?**

    ……..

6. **How does ZICTA communicate and educate the public about the risks of cyber threats in digital financial platforms?**

    ……..

7. **Please provide information on any partnerships ZICTA has with digital financial platform providers in the area of cyber security.**

    ……..

8. **In your assessment, how would you rate the level of cyber threats in Zambia's digital financial services sector on a scale of 1 (Very Low) to 5 (Very High)?**

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

9. **On a scale of 1 (Not Satisfied) to 5 (Very Satisfied), how would you rate ZICTA's efforts and initiatives in maintaining the security of digital financial platforms in Zambia?**
    - ☐ 1
    - ☐ 2
    - ☐ 3
    - ☐ 4
    - ☐ 5
10. **What are the main challenges ZICTA faces in ensuring cyber security in the digital financial services sector?**

    ……..

The end, Thank you

SECTION A: DEMOGRAPHIC DATA

1. **Organization Type**:
    - ☐ Mobile Service Provider (MTN)
    - ☐ Bank
    - ☐ Mobile Service Provider (AIRTEL)
    - ☐ Other (Please specify) _____
2. **Position in the Organization**:
    - ☐ Executive (e.g., CEO, Director)
    - ☐ Middle Management

- ☐ Entry-Level Management
- ☐ Staff (Non-Management)
- ☐ Other (Please specify) _____

3. **Years in the Organization**:
    - ☐ Less than 1 year
    - ☐ 1 - 5 years
    - ☐ 6 - 10 years
    - ☐ More than 10 years
4. Digital financial products/services offered by your organisation

- 1. Internet banking
- 2. Mobile money/banking
- 3. E-wallet
- 4. E-Payment system

SECTION B: SUBSCRIBERS AND CYBER ATTACKS (RESPONSES FROM THE PROVIDERS)

Please provide the following information:

1. **Approximate Number of Subscribers/Users in your Digital Financial Platform**:
    - ☐ Less than 50,000
    - ☐ 50,000 - 100,000
    - ☐ 100,000 - 500,000
    - ☐ 500,000 - 1 million
    - ☐ More than 1 million

2. **Approximate Number of Reported Cyber Attacks in the Last Year**:
    - ☐ None
    - ☐ 1 - 10
    - ☐ 11 - 50
    - ☐ 51 - 100
    - ☐ More than 100

SECTION C: CYBERSECURITY

Using the 5-point Likert scale (1- Strongly Disagree, 2- Disagree, 3- Neutral, 4- Agree, 5- Strongly Agree), please rate the following statements:

1. Our organization has a robust and effective cybersecurity strategy in place.

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

2. Our organization allocates sufficient resources to improve and maintain cybersecurity.

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4

- ☐ 5

3. Our organization has had to significantly increase cybersecurity measures due to rising cyber threats.

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

4. Our organization has successfully prevented most cyber threats.

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

5. Our organization promptly addresses reported cases of cyber threats.

- ☐ 1
- ☐ 2
- ☐ 3

- ☐ 4
- ☐ 5

6. We regularly update our subscribers/users on cybersecurity measures and cyber threats.

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

7. Our subscribers/users are adequately informed on how to protect themselves from cyber threats.

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

8. The regulatory guidelines from ZICTA have helped improve our cybersecurity measures.

- ☐ 1
- ☐ 2

- ☐ 3
- ☐ 4
- ☐ 5

9. We have a dedicated team that constantly monitors and manages cybersecurity risks.

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

10. Cyber threats pose a significant risk to our digital financial services

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

11. Our organization has seen an increase in the uptake of digital financial services

- ☐ 1
- ☐ 2
- ☐ 3

- ☐ 4
- ☐ 5