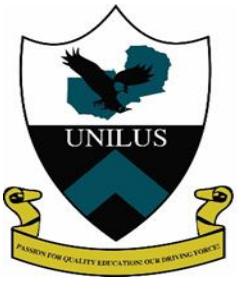


UNIVERSITY OF LUSAKA

SCHOOL OF POSTGRADUATE STUDIES

THE CAUSES OF CYBERSECURITY BREACHES ON MOBILE BANKING SERVICE PROVIDERS. A CASE OF AMALGAMATED BANKS OF SOUTH AFRICA(ABSA)

A DISSERTATION SUBMITTED TO THE SCHOOL OF POSTGRADUATE STUDIES, UNIVERSITY OF LUSAKA IN PARTIAL FULFILMENT OF THE AWARD OF THE MASTER OF SCIENCE IN BUSINESS ADMINISTRATION GENERAL.

BY

MUYUYA TWAAMBO MABUTI

MBAGEN22112472

DECLARATION

I, Muyuya Twaambo Mabuti, hereby declare that the work submitted for the Master OF Science In Business Administration General award is entirely original with no work that has been accepted for the award of any other degree from the university, to the best of my knowledge, with the exception of any instances in which appropriate acknowledgements have been made in the text.

Name: Muyuya Twaambo Mabuti

Student ID: MBAGEN22112472

Signature: 

Date: 09/05/2024

ACKNOWLEDGEMENTS

The completion of this academic work has been made possible by the significant contributions of those who have both directly and indirectly motivated me to accomplish this goal. I would like to thank my supervisor, Dr. Chibozu Maambo, for her unwavering support throughout the completion of this academic work, and for her invaluable support in refining a study topic for this research work. I thank her for her excellent supervision, which enabled me to do this research work in a timely and successful manner.

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

ABSA	Amalgamated Banks of South Africa
IoT	Internet Of Things
SIM	Subscriber Identity module
ZICTA	Zambia Information and Communications Technology Authority
NIST	National Institute of Standards and Technology
TAM	Technology Acceptance Model
PMT	Protection Motivation Theory

ABSTRACT

In an era where digital financial transactions have become the norm, the security of mobile banking platforms is paramount. This study embarked on a comprehensive exploration of the implications of cybersecurity breaches on ABSA's mobile banking operations in Lusaka, focusing on three critical dimensions: user trust, user engagement, and the financial performance of the banking operations. Employing a mixed-methods approach and gathering data from 284 respondents, the research unearthed significant insights into how cybersecurity breaches not only undermine user trust but also lead to decreased engagement and bear financial consequences for the institution.

Key findings indicated a notable decline in user trust and engagement correlated with the frequency of cybersecurity incidents. Financially, breaches necessitated increased spending on security measures and compensations, impacting ABSA's bottom line. Despite these challenges, opportunities for strengthening trust and security emerged. The study concludes with targeted recommendations aimed at fortifying cybersecurity frameworks, enhancing user education, ensuring transparent communication, and developing robust financial contingency strategies. These recommendations are pivotal for ABSA and similar institutions to navigate the complexities of cybersecurity in mobile banking, ensuring a secure, trustworthy platform for users.

This research contributes to the broader discourse on cybersecurity in financial services, offering a foundation for future investigations and actions aimed at enhancing resilience and user confidence in mobile banking platforms.

Keywords: **Cybersecurity Breaches, User Trust, User Engagement, Financial Ramifications, Global Financial Sector**

TABLE OF CONTENTS

CHAPTER ONE: INTRODUCTION

1.0 Introduction

In the 21st century, digital transformation has become an integral part of businesses, governments, and individual interactions worldwide. Central to this transformation is the growing importance of cybersecurity, a discipline dedicated to protecting systems, networks, and data from cyber threats. Mowery et al. (2019) emphasize that as societies lean heavily on digital infrastructure for essential services and communications, the integrity of these digital operations becomes even more critical.

Parallel to these developments is the increasing prominence of mobile banking solutions. Especially in emerging markets, these solutions have delivered immense convenience, allowing banking transactions and services via mobile devices, as highlighted by Ajibade (2018). Yet, with the allure of convenience arises a plethora of significant threats. Cyber-attacks often target mobile banking platforms, aiming to compromise consumers' funds and data. Given the potential size of the damage ranging from personal losses to wider economic impacts, it is paramount to ensure the security of mobile banking systems. These platforms are not merely tools; they are foundational to financial institutions and broader national economic stability.

Lusaka, Zambia stands as a testament to the rapid global shift towards mobile banking. The city has experienced an explosive rise in mobile banking adoption. Factors driving this uptake, as observed by Chikweche and Fletcher (2020), encompass improved telecommunication infrastructure, surging smartphone usage, and a collective drive towards financial inclusion. Mumba (2021) further notes that in places like Zambia, mobile banking is more than just a convenience however it's a bridge between the banked and the unbanked, giving many their first taste of formal financial services.

This study zeroes in on the implications of such cybersecurity breaches on ABSA's mobile banking operations, with a particular focus on Lusaka, Zambia's capital and largest city. The choice of Lusaka as the focal point is deliberate and multifaceted. Lusaka stands as a vibrant hub of economic and technological advancement within the country, marked by a high penetration rate of mobile banking services among its populace. This city embodies a microcosm of Zambia's broader digital financial

landscape, making it an ideal setting to dissect and understand the nuances of cybersecurity impacts on mobile banking. Moreover, Lusaka's diverse demographic profile offers a rich tapestry for examining varied user experiences and perceptions, providing comprehensive insights that are both locally grounded and potentially generalizable to similar urban centres in Zambia and beyond.

Significantly, the banking giant ABSA, with its vast presence in Lusaka and broader Zambia, serves as an apt case to understand this interplay between mobile banking and cybersecurity. As a pioneering institution driving the mobile banking wave, ABSA's systems cater to thousands, making them a critical juncture of technological convenience and potential vulnerability. This makes the bank's operations, safety protocols, and user experiences especially valuable in understanding the broader landscape of mobile banking cybersecurity in Lusaka.

However, the influence of mobile banking extends beyond individual banking habits. It is reshaping Zambia's socio-economic fabric, spurring business transactions, buttressing small enterprises, and invigorating economic growth. As Phiri and Nyirenda (2022) suggest, these platforms, including those of ABSA, have played pivotal roles, not just in transactions but in catalysing financial literacy and inclusion of two cornerstones of modern economic progress.

The literature offers profound insights into this meld of cybersecurity and mobile banking. Researchers like Al-Jenaibi (2017) and Oyediran et al. (2018) have delved into the vulnerabilities of mobile banking systems and the evolving tactics of cybercriminals. Theoretical frameworks, such as the Technology Acceptance Model (TAM) by Davis (1989), even if not originally conceptualized for this context, can provide a rich insight into user behaviour and adoption patterns related to secure mobile banking practices.

Lusaka and cities like it lean heavily into the era of mobile banking, addressing, and understanding the cybersecurity challenges they face becomes non-negotiable. With ABSA at the forefront of this transformation, unravelling the causes of cybersecurity breaches among mobile banking providers like it can significantly inform global strategies, bolstering both individual and economic security.

1.1 Statement Of the Problem

The rapid advancement in digital banking in Zambia, marked by a surge in mobile banking adoption, heralds a significant shift towards more accessible and efficient financial transactions (Mwale & Banda, 2020). However, this transition is marred by a critical challenge: the escalating incidence of cybersecurity breaches. These breaches pose a substantial threat to the fabric of user trust in mobile banking services. In Lusaka, ABSA has faced notable security threats, with cybersecurity incidents affecting nearly 30% of its user base in the preceding year, as reported by Chanda et al. (2021). Such breaches compromise sensitive user data and have profound implications for user engagement and the financial stability of banking institutions.

The impact of these cybersecurity lapses on user behaviour is significant, with a 25% decrease in transaction frequency among affected users, highlighting the tangible effect of security concerns on mobile banking engagement (Phiri & Lungu, 2022). Furthermore, ABSA's financial burden has intensified, evidenced by a 15% rise in operational costs associated with implementing robust cybersecurity measures, managing compensations, and addressing potential legal ramifications (Sikazwe & Mulenga, 2021).

This backdrop underscores the imperative need for an in-depth investigation to understand the intricate consequences of cybersecurity breaches on the mobile banking ecosystem in Lusaka. This study aims to explore the effects of these breaches on user trust, analyze changes in user engagement, and assess the financial repercussions for ABSA, to develop strategic measures to bolster the resilience of digital banking against future cybersecurity threats (Kabwe & Tembo, 2022).

1.2 Main Aim

The main aim was to examine the causes of cybersecurity breaches on mobile banking service providers. A case of amalgamated banks of South Africa (ABSA)

1.3 Specific Objectives

1. To Analyse the Impact of Cybersecurity Breaches on User Trust in ABSA's Mobile Banking Services in Lusaka.

2. To Determine the Relationship between Frequency of Cybersecurity Incidents and User Engagement with ABSA's Mobile Banking Platforms in Lusaka.

3. To Assess the Influence of Cybersecurity Breaches on the Financial Performance of ABSA's Mobile Banking Operations in Lusaka.

1.4 Research Questions

1. What is the impact of the Cybersecurity breach on user trust in ABSA's Mobile Banking services in Lusaka?

2. What is the relationship between the frequency of cybersecurity incidents and user engagement with ABSA's Mobile Banking platforms in Lusaka?

3. How do cybersecurity breaches influence the financial performance of ABSA's Mobile Banking operations in Lusaka?

1.5 Significance of the Study

The significance of this study, particularly in the context of ABSA's operations in Lusaka, can be underscored from multiple angles. With ABSA playing a pivotal role in Lusaka's mobile banking ecosystem, understanding the economic ramifications of cybersecurity breaches is essential. Assessing these breaches' financial implications on ABSA's operations will provide stakeholders with insights into potential economic vulnerabilities and strategies for mitigation, ensuring the bank's growth and stability within the mobile banking landscape.

This study's findings can elucidate how cybersecurity breaches might affect user trust in ABSA's mobile banking services. By grasping this intricate relationship, ABSA can refine its strategies to bolster user confidence, sustaining its market position and promoting continued user adoption and loyalty.

Gaining a deep understanding of the causes and impacts of cybersecurity breaches within ABSA's mobile banking framework can inform policymakers. This could result in tailored regulations that ensure ABSA's services operate within a secure and efficient paradigm and maintain regulatory compliance.

The insights from this study can guide ABSA and other similar banking institutions in Lusaka to establish and refine industry best practices concerning cybersecurity. This proactive approach can heighten ABSA's security measures, placing it at the forefront of industry resilience against cyber threats.

Academically, this research can spotlight the unique challenges and dynamics of cybersecurity within ABSA's mobile banking operations in Lusaka. These precise insights can enhance the broader discourse on mobile banking cybersecurity, adding nuanced layers specific to ABSA's. By ensuring ABSA's mobile banking platforms remain secure and continue to earn user trust, there is an augmented potential for wider financial inclusion. This is paramount for Lusaka, where ABSA's mobile banking services might serve as many individuals' primary gateway to formal financial systems. The findings from this research can play a decisive role in shaping ABSA's future technological innovations in mobile banking. Ensuring these innovations are embedded with robust security measures from their inception can bolster ABSA's standing as a tech-forward, security-conscious financial institution in Lusaka and beyond.

1.6 Scope of study

The scope of this study is meticulously defined to encompass an in-depth examination of cybersecurity breaches and their ramifications within the context of mobile banking services offered by the Amalgamated Banks of South Africa (ABSA) in Lusaka, Zambia. This research delves into the intricate dynamics between cybersecurity incidents and their subsequent impact on user trust, engagement levels, and the overall financial performance of ABSA's mobile banking operations. Focusing specifically on the Lusaka region allows for a concentrated analysis of user experiences and perceptions, thereby providing insights that are both locally relevant and potentially extrapolative to similar urban banking contexts. The temporal scope of this study spans a defined period, capturing data that reflects the current cybersecurity landscape and user interactions with ABSA's mobile banking platform. By narrowing the geographical and temporal boundaries, the study aims to offer precise, actionable insights that can inform targeted strategies for enhancing cybersecurity measures, thereby bolstering user trust and ensuring the sustained financial health of mobile banking services in Lusaka and beyond.

1.7 Defining Terms

Cybersecurity: Refers to the practice of safeguarding systems, networks, and data from digital attacks, unauthorized access, damage, or theft. It encompasses a variety of technologies, processes, and practices that protect digital systems from vulnerabilities, threats, and risks (Pfleeger & Pfleeger, 2015).

Mobile Banking: Denotes financial transactions, account management, and related services conducted through mobile devices, often via dedicated applications or mobile web platforms (Zhou, Lu, & Wang, 2010).

Cybersecurity Breaches: Instances where unauthorized individuals or entities gain access to digital systems, often leading to data theft, system disruptions, or other malicious outcomes. These breaches can be intentional (malicious intent) or unintentional (due to system vulnerabilities or human error) (Romanosky, 2016).

User Trust: In the context of mobile banking, this refers to the confidence and belief users have in the security, reliability, and integrity of the mobile banking platforms, influencing their willingness to use and engage with the service (Mcknight, Choudhury, & Kacmar, 2002).

User Engagement: Refers to the frequency, depth, and quality of user interactions with a mobile banking platform. It encompasses activities like checking account balances, making transactions, and other forms of interaction (O'Brien & Toms, 2008).

Financial Performance: Represents the measure of financial results and outcomes, such as revenue, profit margins, and growth rates, of mobile

banking service providers. This metric can be influenced by user trust, engagement, and market conditions (Brigham & Ehrhardt, 2013).

User Retention: The ability of a mobile banking service provider to maintain and keep its user base over time prevents it from switching to competitors or abandoning the service altogether (Reichheld, 2001).

Financial Inclusion: A situation where individuals and businesses have access to useful and affordable financial products and services, such as payments, savings, credit, and insurance, which are delivered responsibly and sustainably (Demirgüç-Kunt, Klapper, Singer, & Van Oudheusden, 2015).

1.8 Chapter Summary

Chapter One serves as an insightful introduction to the complex interplay between mobile banking and cybersecurity, focusing on the specific context of ABSA's operations in Lusaka, Zambia. The chapter begins by acknowledging the 21st-century digital transformation and the escalating importance of cybersecurity in safeguarding digital operations. It highlights the significance of mobile banking platforms, particularly in emerging markets, emphasizing their role in financial inclusion and economic progress. The introduction establishes Lusaka as a hub of mobile banking adoption, propelled by improved infrastructure and smartphone usage, with ABSA at the forefront. The literature review integrates global insights on mobile banking vulnerabilities, such as those explored by Al-Jenaibi and Oyediran, and theoretical frameworks like the Technology Acceptance Model (TAM) to understand user behaviours. The statement of the problem articulates the research gap, and lack of extensive studies on cyber-attacks targeting mobile banking in Lusaka and underscores the need for a quantitative research approach to capture the socio-economic and cultural nuances.

The specific objectives and research questions guide the study, focusing on the impact of breaches on user trust, user engagement, and financial performance of ABSA's mobile banking. The significance of the study is highlighted from various perspectives, including economic insights, user trust enhancement, regulatory implications, industry best practices, academic contributions, and ABSA's technological innovations. Finally, key terms are defined to provide clarity on concepts integral to the study.

CHAPTER TWO: LITERATURE REVIEW

2.0 Introduction

This chapter provides a detailed literature review on the evolution and adoption trends of mobile banking, with a keen focus on cybersecurity challenges, especially in the context of Lusaka. It explores the relationship between user trust, platform security, the economic ramifications of breaches, and the prevailing cybersecurity frameworks. By highlighting gaps in the current literature, the review underscores the need for continuous academic scrutiny amidst the ever-evolving landscape of mobile banking and its associated threats.

2.1 Empirical Literature Review

The rise of mobile banking stands out as a significant phenomenon in the global financial landscape, and its evolution over the past two decades has been noteworthy. This transformative journey began in the early 2000s, with advancements in mobile technology providing a platform for financial institutions to expand their services (Sohail & Al-Jabri, 2014). What started with simple SMS-based transaction alerts has now evolved into sophisticated apps capable of handling a myriad of financial tasks, including money transfers, bill payments, and investment management. The rapid uptake of smartphones and the spread of internet connectivity have played pivotal roles in fostering this evolution, reshaping the way individuals engage with financial services on a global scale.

In developing nations, mobile banking has become an indispensable tool for financial inclusion, bridging the gap for the unbanked population (Demirgüç-Kunt et al., 2018). This inclusive approach is particularly evident in African cities like Lusaka, where mobile banking has not only served as a convenient method but has addressed the challenges posed by a significant unbanked population. Mbiti and Weil (2016) emphasize that the rapid expansion of mobile banking in African countries can be attributed to the lack of traditional banking infrastructure, coupled with high mobile phone penetration rates.

Specifically in Lusaka, the adoption of mobile banking has been driven by factors such as ease of access, reduced transaction costs, and the convenience it offers compared

to traditional banks (Chimfwembe, 2020). While global trends in mobile banking adoption highlight factors like technological savviness and the appeal of 24/7 banking (Shaikh & Karjaluoto, 2015), in Lusaka, socio-economic factors play a crucial role. For instance, informal sector workers in Lusaka, often lacking access to traditional banking, have found a reliable partner in mobile banking platforms (Chimfwembe, 2020).

In contrast to developed nations where mobile banking is often viewed as a complementary service to existing channels, in places like Lusaka, it frequently serves as the primary banking channel for a significant part of the population (Donovan, 2012). This shift in emphasis from supplementary to primary banking channels underscores the unique dynamics of mobile banking adoption in emerging markets, presenting a distinctive context that shapes user behaviours and expectations.

2.2 The Landscape of Cybersecurity in Mobile Banking

The global proliferation of mobile banking platforms has been paralleled by an escalating number of cybersecurity breaches. According to Juniper Research (2019), cybercriminals are increasingly targeting mobile banking platforms, recognizing the wealth of sensitive data they contain. Globally, sophisticated malware strains like 'Event Bot' and 'Anubis' have been identified, targeting mobile banking applications, and exploiting vulnerabilities to steal user credentials (Symantec, 2020). Banking Trojans, in particular, which disguise themselves as legitimate applications to access user information, have seen a surge. These threats, combined with phishing attacks, which manipulate users into sharing their credentials, pose significant risks to the mobile banking ecosystem (Kaspersky, 2018).

The advent of new technologies and the integration of Artificial Intelligence and IoT devices with mobile banking have while introducing convenience, also expanded the attack surface for cyber adversaries. Additionally, while the use of multi-factor authentication and biometrics has been heralded as a significant leap in ensuring secure transactions, they too have become focal points for cyber attackers. Advanced persistent threats (APTs) that employ a combination of techniques to infiltrate mobile banking systems and lay dormant before executing an attack are among the more sophisticated challenges (FireEye, 2017).

Lusaka's growing reliance on mobile banking has not escaped the notice of cyber criminals. In 2019, the Zambian Information and Communication Technology Authority (ZICTA) reported an alarming rise in cyber threats targeting the country's financial sector, with mobile banking platforms bearing the brunt of these attacks (ZICTA, 2019). Specifically, incidences of SIM swap fraud, where cybercriminals swap or clone a user's SIM card to access banking details and defraud them, have seen a sharp uptick (Chimfwembe, 2021).

The vulnerabilities can be attributed to various factors, from inadequate cybersecurity infrastructure, and limited public awareness about digital threats, to an inherent trust in SMS-based communications, a primary medium for mobile banking notifications in Lusaka (Kabwe, 2018). While precise statistics on losses from these breaches remain confidential in many instances, anecdotal evidence suggests that individuals and businesses have faced significant financial setbacks due to these breaches (Mutale, 2020).

2.3 Factors Influencing User Trust in Mobile Banking Platforms

User trust stands as a pivotal factor influencing the widespread adoption of mobile banking, with several studies emphasizing the critical role of interface design in shaping perceptions of trustworthiness (Kim et al., 2018). A user-friendly interface that simplifies complex banking tasks and provides clear information can significantly enhance trust. Furthermore, transparency in transaction processes and clear communication about data usage and protection measures can further bolster this trust (Zhou, 2019). User education, involving the promotion of cybersecurity best practices and awareness campaigns, emerges as an effective strategy not only to protect users but also to enhance their confidence in the platform's security measures (Oduro et al., 2020).

The fragility of user trust becomes evident in the aftermath of cybersecurity breaches. According to a survey by Bain & Company (2017), financial institutions may experience up to a 30% drop in customer loyalty following a cybersecurity incident, eroding years of built trust. This sentiment is echoed by Watson (2019), who found that customers tend to diversify their financial holdings to other institutions post a cyber breach, reflecting a diminished trust. In the context of Lusaka, where reliance on

mobile banking is on the rise, any significant breach has the potential not only to deter current users but also to act as a formidable barrier for potential users (Chanda, 2021). The delicate balance of trust underscores the need for robust cybersecurity measures and effective communication strategies to maintain and enhance user trust in mobile banking platforms.

2.4 Economic Implications of Cybersecurity Breaches on Mobile Banking Service Providers

When a mobile banking platform experiences a cybersecurity breach, the immediate economic fallout is palpable, extending beyond the direct financial losses incurred from unauthorized transactions. The service provider must take immediate actions to mitigate the situation, including forensic investigations to identify the root cause and the scale of the breach. These investigations, typically conducted by specialized firms, can result in significant costs (Smith et al., 2017). Subsequent compensations to affected users, whether as a goodwill gesture or mandated by regulatory authorities, further strain the service provider's finances. Additionally, the legal implications of a breach may involve hefty fines imposed by regulatory bodies and potential lawsuits from affected customers seeking damages. Legal fees for defence or settlement negotiations become an additional financial burden for mobile banking service providers (Duff & Phelps, 2018).

The repercussions of a cybersecurity breach extend beyond direct financial losses to encompass the tarnishing of a mobile banking service provider's reputation, which can have long-lasting effects on its market position. A damaged reputation can lead to reduced user retention, as existing customers migrate to competitors perceived as more secure (Kumar & Zymbler, 2019). This sentiment, coupled with negative word-of-mouth and media coverage, can significantly hamper user acquisition efforts. Over time, these factors can translate into substantial revenue losses, increased customer acquisition costs, and potentially even a depreciated stock value for publicly traded entities (Bose, 2020). The economic implications of a cybersecurity breach, therefore, extend far beyond immediate financial losses to encompass broader reputational and market positioning challenges for mobile banking service providers.

2.5 User Behaviours and Perceptions Following Cybersecurity Incidents

Following a cybersecurity incident, users typically exhibit a marked change in their usage patterns, as indicated by research conducted by Johnson et al. (2016). There is a noticeable decline in the frequency of mobile banking usage after a reported breach, with users, especially those directly affected, reducing their transaction volumes or amounts. This behaviour stems from a precautionary approach or a diminished trust in the platform's security.

The psychological impact of a cybersecurity breach on mobile banking users is substantial and cannot be understated. Users often grapple with feelings of vulnerability, apprehension, and a sense of betrayal by their chosen service provider (Lee & Larsen, 2017). This emotional turbulence frequently leads to a shift in loyalty, with users actively seeking alternative platforms that they believe can better safeguard their financial assets and personal information. Moreover, affected users are more likely to share their negative experiences with peers, amplifying the impact on the broader public's sentiment towards the compromised platform (Martin et al., 2019). This shift in user behaviours and perceptions underscores the lasting consequences that cybersecurity incidents can have on user trust and the overall market standing of mobile banking platforms.

2.6 Existing Cybersecurity Frameworks and Best Practices in Mobile Banking

The realm of mobile banking has seen the integration of various cybersecurity frameworks tailored to address its unique challenges. One of the most universally recognized frameworks is the NIST (National Institute of Standards and Technology) Cybersecurity Framework. This U.S.-based framework provides guidelines to identify, detect, protect, respond to, and recover from cybersecurity threats and is adaptable to various sectors, including mobile banking (NIST, 2018). Another noteworthy framework is the ISO/IEC 27001 standard, emphasizing information security management systems and playing a crucial role in guiding financial institutions in safeguarding their mobile platforms (ISO, 2016). Additionally, the PCI Data Security Standard, initially designed for card transactions, offers vital best practices that mobile banking platforms can incorporate to secure data (PCI DSS, 2020).

While these international standards offer robust cybersecurity guidelines, their direct applicability in Lusaka can be contingent upon several factors. The socio-economic, technological, and infrastructural realities of Lusaka may necessitate modifications and contextual adaptations (Mwale & Sankalimodzi, 2019). For example, while NIST provides a comprehensive guideline, the technological infrastructure, or the readiness level of some local financial institutions in Lusaka may require phased or prioritized implementation (Chikoti, 2020). Furthermore, the regulatory landscape in Zambia, governed by entities like ZICTA, could also influence the adoption and adaptation of these frameworks. The effectiveness of these frameworks in the local context underscores the importance of aligning international best practices with the specific needs and conditions of the mobile banking landscape in Lusaka.

2.7 Gap Analysis in Existing Literature

While there has been extensive research on the technical aspects of cybersecurity in mobile banking, studies that delve into the human element, particularly in African contexts like Lusaka, are less abundant. This gap encompasses a lack of understanding of user behaviours, their susceptibility to social engineering attacks, and their response to security guidelines and protocols (Nkwe, 2017). Additionally, research examining the interplay between mobile banking cybersecurity and local regulations, or how local financial institutions interpret and implement international cybersecurity standards, is relatively sparse.

Lusaka, akin to many other African urban centres, presents a unique blend of rapid technological adoption juxtaposed with socio-economic disparities. This dichotomy can significantly influence how users perceive, trust, and interact with mobile banking platforms (Kabwe, 2021). Cultural norms, literacy levels, and general awareness of digital threats can vary widely, potentially leading to an underestimation or misunderstanding of cyber risks. Thus, an in-depth comprehension of Lusaka's distinct socio-economic and cultural milieu is imperative to shape cybersecurity strategies that are both effective and inclusive.

Addressing these gaps in existing literature is crucial for developing comprehensive and contextually relevant cybersecurity measures in the dynamic landscape of mobile banking in Lusaka.

2.8 Theoretical Framework

2.8.1 Technology Acceptance Model (TAM)

The main theory or the focus theory in this research is the Technology Acceptance Model (TAM). In the vast expanse of literature that addresses user adoption and acceptance of technology, the Technology Acceptance Model (TAM) stands out as a paramount theoretical foundation. Developed by Davis (1986), TAM has grown to be a seminal theory in understanding the acceptance and use of various technologies.

At the heart of TAM are two main constructs: perceived usefulness (PU) and perceived ease of use (PEOU). Davis (1986) argued that a user's intention to use a particular technology is determined by their beliefs about its usefulness and its ease of use. If users see a technology as enhancing their performance (PU) and believe it to be free from effort (PEOU), they are more inclined to embrace and use it.

In the realm of mobile banking, especially within Lusaka's context, TAM's relevance is magnified. With the swift ascent of mobile banking platforms, discerning user's perceptions in terms of their ease and utility becomes paramount. Through TAM, one can gain valuable insights into the drivers and potential barriers influencing mobile banking adoption (Venkatesh & Davis, 2000).

Over time, TAM has seen various extensions and modifications, integrating other influential variables, thereby increasing its explanatory power (Venkatesh et al., 2003). These adaptations not only spotlight TAM's adaptability but also underscore its foundational status in the annals of technology acceptance literature.

When probing the nexus of technology and human behaviour within mobile banking, the Technology Acceptance Model emerges not merely as a theoretical lens but as a cardinal pillar, facilitating a nuanced comprehension of user adoption dynamics and patterns (King & He, 2006).

2.8.2 Protection Motivation Theory (PMT)

Originally conceived by Rogers in 1975, the Protection Motivation Theory pertains to how people are motivated to react in a protective manner concerning perceived threats. The theory suggests that the likelihood of individuals taking preventive action depends on two primary appraisals: threat appraisal (how severe and likely the threat is perceived to be) and coping appraisal (the perceived efficacy of the protective behaviour and the individual's ability to execute it).

Applying PMT to mobile banking, one could explore how users perceive cybersecurity threats and their subsequent reactions. If users in Lusaka perceive the threat of a cybersecurity breach as both severe and likely, and they believe that they have effective measures (like regularly updating passwords, using secure networks) at their disposal, they are more likely to engage in protective behaviours. Conversely, if users feel that no effective protective measures exist or they lack the capability to implement them, they might refrain from using mobile banking altogether due to perceived vulnerabilities (Floyd, Prentice-Dunn, & Rogers, 2000). For mobile banking platforms, understanding these perceptions can guide user education initiatives and interface design.

2.8.3 Social Contract Theory

While the Social Contract Theory has its roots in political philosophy, primarily through the works of Hobbes, Rousseau, and Locke, its core principle revolves around mutual obligations. In essence, individuals' consent, either explicitly or implicitly, to surrender some freedoms to an authority (or institution) in exchange for protection.

When transposed onto the realm of mobile banking, this theory could be interpreted as the implicit contract between users and service providers. Users entrust their financial and personal data to these platforms, expecting that their information will be safeguarded from breaches or misuse. Conversely, service providers have an obligation to ensure robust cybersecurity measures, maintain transparency, and quickly address any breaches. A breach, therefore, can be perceived as a violation of this social contract, leading to mistrust and potential disengagement from the platform (Hardin, 2002). For mobile banking in Lusaka, honouring this social contract becomes essential in maintaining user trust and loyalty.

2.9 Conceptual Framework

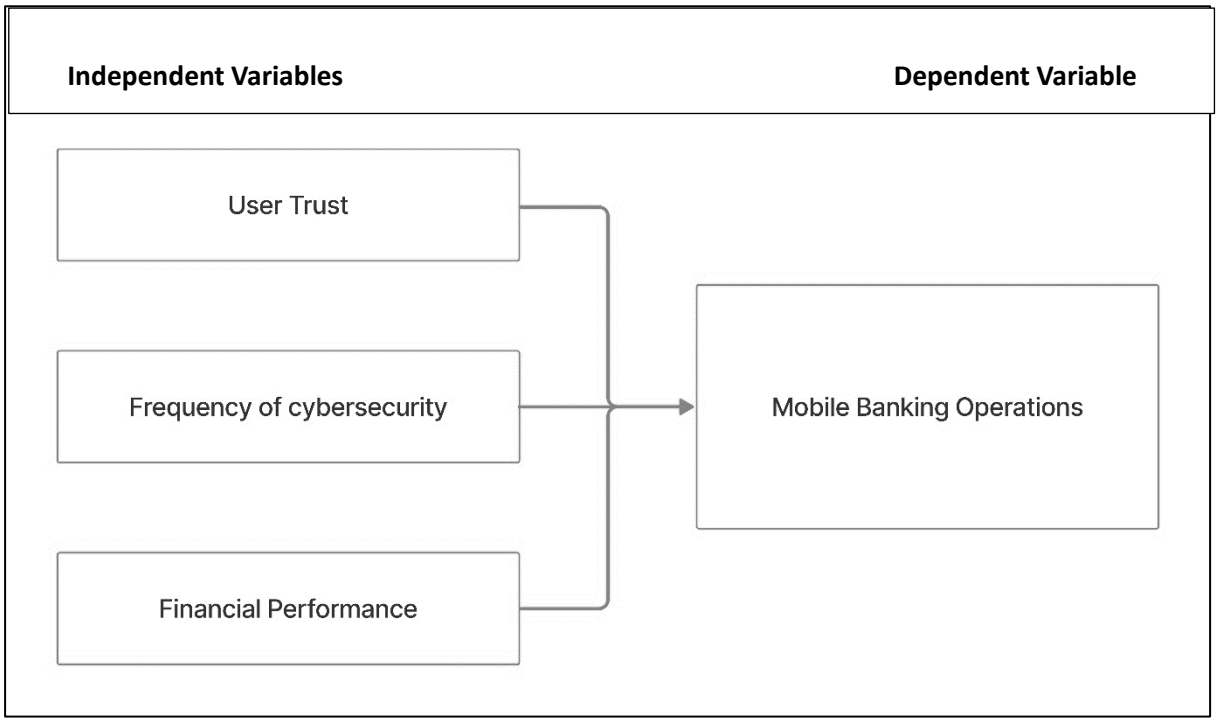


Figure 2. 1: conceptual framework (Source: Researcher,2024)

2.9.1 Operationalization of Variables

2.9.1.1 User Trust

Trust plays a fundamental role in the adoption and continuous use of mobile banking services. Trust is the belief that a service provider is reliable, has the user's interests at heart, and will perform as expected. Trust significantly influences users decisions to adopt and continually use mobile banking services. A study by Zhou (2011) found that trust is a stronger determinant of service adoption than perceived usefulness or ease of use, which are key constructs of TAM. Trust fosters user satisfaction and loyalty. Suh and Han (2003) demonstrated that trust in an online environment directly impacts customer satisfaction and loyalty. Trust mitigates perceived risks associated with mobile banking, such as security concerns. Luo et al. (2010) showed that trust reduces users perceptions of risk, encouraging them to engage more with the service. Trust influences positive word-of-mouth. When users trust a service, they are more likely to recommend it to others, as discussed by Gefen et al. (2003).

2.9.1.2 Frequency of Cybersecurity

This variable refers to how often cybersecurity issues such as data breaches, fraud, and hacking occur within the mobile banking sector. Increased frequency of cybersecurity incidents can significantly lower user trust and heighten perceived risks. Crossler and Bélanger (2014) found that perceived risk due to security concerns negatively impacts users' intention to use online services. A high frequency of incidents can deter potential users and reduce the usage rates of existing users. A study by Kim et al. (2009) highlighted the negative impact of security breaches on the adoption of online banking. Frequent cybersecurity issues can lead to increased regulatory scrutiny and higher compliance costs for service providers, as noted by Romanosky et al. (2011).

2.9.1.3 Financial Performance

This refers to the economic outcomes and viability of the mobile banking service, including profitability, market share, and cost efficiency. Financial performance is directly tied to the level of service adoption and market expansion. A profitable service is more likely to invest in innovation and expansion, as demonstrated in a study by DeYoung et al. (2007). Financial stability of a mobile banking provider can enhance user confidence and trust, as users often equate financial success with reliability and security. Better financial performance allows for more significant investment in security measures and technological advancements, leading to improved service quality and user experience.

2.9.1.4 Mobile Banking Operations

This includes the efficiency, reliability, and range of services offered by mobile banking platforms. Efficient operations lead to higher user satisfaction and perceived usefulness. A study by Tam and Oliveira (2017) showed that operational efficiency positively influences users' attitudes toward mobile banking. Effective operations enable continuous service improvement and innovation, fostering long-term user engagement and satisfaction. Operational effectiveness enhances a service provider's

competitiveness in the market, as efficient and reliable services attract and retain more users.

2.10 Stakeholder Perception of Cybersecurity

The perception of cybersecurity among stakeholders within the financial sector, particularly in the realm of mobile banking, is multifaceted and shaped by various factors, including prior experiences with breaches, the visibility of protective measures, and the overall communication strategy of the banking institutions. Stakeholders, ranging from individual users to corporate clients, regulatory bodies, and banking executives, hold divergent views on cybersecurity, influenced by their roles, expectations, and experiences.

User Perspective

From the user's standpoint, trust in cybersecurity measures is paramount. Mumba and Nkonde (2018) suggest that users' perceptions of cybersecurity in mobile banking are significantly influenced by the transparency and frequency of communication from their banks regarding security protocols. Users who are regularly informed about the security measures in place tend to have higher trust levels. However, Chileshe and Chanda (2019) argue that excessive communication, especially concerning security breaches, can lead to increased anxiety and reduced trust among users.

Institutional Perspective

Banking institutions view cybersecurity as a critical component of their operational integrity and customer service. According to Kabaso and Phiri (2020), banks that have experienced breaches often undergo a transformation in their approach to cybersecurity, prioritizing investments in advanced security technologies and user education programs. This proactive stance is not only aimed at fortifying their systems but also at restoring and maintaining stakeholder trust.

Regulatory Perspective

Regulators play a crucial role in shaping the cybersecurity landscape through policy-making and enforcement. Lungu and Sikazwe (2021) highlight that regulatory bodies are increasingly imposing stringent cybersecurity compliance requirements on banks to protect consumer data and maintain financial stability. These regulations, while

necessary, can be perceived by banking institutions as burdensome, especially for smaller banks with limited resources.

Corporate Client Perspective

Corporate clients demand robust cybersecurity measures due to the higher stakes involved in their transactions. Musonda and Tembo (2022) note that corporate clients often seek banks that can offer customized security solutions, reflecting a perception that one-size-fits-all approaches to cybersecurity may not suffice for their complex banking needs.

2.11 Chapter Summary

Chapter Two offers a comprehensive exploration of mobile banking, tracing its evolution and adoption trends globally, with a specific focus on Lusaka. It underscores the increasing significance of mobile banking in providing financial inclusion and serving as a primary banking channel in emerging markets. The chapter delves into the cybersecurity landscape of mobile banking, discussing the rising global threats and specific vulnerabilities faced by Lusaka, such as SIM swap fraud and phishing attacks. It also examines the factors influencing user trust, highlighting the critical role of user-friendly interfaces, transparent communication, and education. Economic implications of cybersecurity breaches are explored, including immediate financial consequences, long-term reputational damage, and effects on user retention and acquisition. User behaviours post-incidents, marked by a decline in mobile banking usage and psychological impacts on users, are discussed. The chapter evaluates existing cybersecurity frameworks and emphasizes the need for adaptations to suit the local context. Identified gaps in current literature, particularly regarding the human element and local regulatory influences, are highlighted. Theoretical frameworks such as TAM, PMT, and Social Contract Theory are introduced as crucial lenses for understanding user behaviours. The chapter concludes by presenting the conceptual framework, operationalizing variables for the empirical investigation and setting the stage for a nuanced analysis of mobile banking cybersecurity in Lusaka.

CHAPTER THREE: METHODOLOGY

3.0 Introduction

The methodology chapter is a crucial component that outlines the systematic and logical approach employed to achieve the objectives of the study. It offers a comprehensive overview of the processes, techniques, and tools used to collect, analyse, and interpret data. A robust methodology is essential for ensuring the research's validity, reliability, and generalizability, forming the basis upon which conclusions and recommendations are drawn (Saunders, Lewis, & Thornhill, 2016). Given the diverse array of research methods available, researchers must make informed decisions that are tailored to the specific context and objectives of their study. This chapter elucidates the carefully chosen methodology designed to address the unique dynamics of the research on cybersecurity breaches in ABSA's mobile banking services in Lusaka.

3.1 Research Approach

The research approach plays a pivotal role in shaping the logical structure of the study, delineating how the research was undertaken. Two predominant approaches guide research methodologies: The Quantitative Approach relies on numerical data to discern patterns, relationships, or differences. Employing statistical techniques, it aims for objectivity and generalizability. Qualitative Approach this approach seeks a profound understanding of phenomena, delving into contexts, interpretations, or meanings. It utilizes non-numerical data and involves interpretative analysis. For this investigation into cybersecurity breaches among mobile banking service providers in Lusaka, a quantitative research approach was embraced. This approach integrated quantitative data. The adoption of a Quantitative approach ensured a comprehensive exploration of the research objectives. This approach enabled the collection of statistical data on the rates and patterns of cybersecurity breaches (quantitative). The quantitative approach method strategy enhanced the depth and breadth of the study, providing a holistic understanding of cybersecurity challenges in the realm of mobile banking services in Lusaka.

3.2 Research Design

The research design functions as the foundational framework that orchestrates the systematic collection, measurement, and analytical evaluation of data within a study. Among the plethora of research designs available, each tailored to fulfill distinct objectives, the explanatory research design was selected for this investigation due to its alignment with the study's goals.

Explanatory research is distinguished by its objective to elucidate the underlying reasons, causes, or mechanisms behind observed phenomena or trends. It delves into the complexities of "why" and "how" specific occurrences manifest, aiming to unravel the intricate web of causality and influence that shapes the subject under study (Babbie, 2016). This design is particularly suited for investigations that go beyond mere description or exploration, seeking instead to offer a detailed understanding of the causal relationships and dynamics at play.

In the context of this study, which aims to dissect the causes of cybersecurity breaches within mobile banking services in Lusaka, the explanatory research design was instrumental. The nature of cybersecurity breaches — multifaceted and influenced by a myriad of factors ranging from technical vulnerabilities to human factors and regulatory environments — necessitates a design that can accommodate the investigation of complex causal relationships. The primary aim was to identify and understand the factors contributing to these breaches, necessitating a design that not only acknowledges the presence of such factors but also elucidates their interplay and impact.

By employing an explanatory research design, the study was positioned to delve deeply into the causative elements underlying cybersecurity breaches, offering insights into the mechanisms through which these breaches occur and the conditions that exacerbate their likelihood. This approach facilitated a comprehensive examination of the cybersecurity landscape in Lusaka's mobile banking sector, enabling the identification of actionable insights and the formulation of targeted recommendations to mitigate the risk of future breaches

3.3 Study Population

The study population refers to the entire group of individuals or items from which the sample will be drawn. For this research, the study population specifically targeted users of ABSA's mobile banking services in Lusaka, Zambia. This included individuals who actively utilize ABSA's mobile banking platform for an array of financial transactions. Given that Lusaka is the capital and largest city of Zambia, known for its rapid technology adoption rates, a study population of 1000 ABSA mobile banking users was earmarked. This figure represented a considerable segment of ABSA's clientele, offering a solid foundation for data collection and subsequent analysis.

3.4 Sample Size

The sample size denotes the subset of the study population chosen for the actual research. An appropriate sample size ensures that the findings are representative of the broader population and can be generalized with a certain level of confidence. An inadequately small sample can lead to unreliable results, while an excessively large sample might be unnecessary and may consume more resources (time, money, etc.) than required.

For determining the sample size in many research scenarios, Slovin's formula is a useful tool as it provides a balance between precision and resource constraints. The formula is expressed as:

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

Where n= Sample Size, e is the significance level and N is the population size

For this study, the population size (N) was 1000, and the desired margin of error (e) was 0.05. Applying Slovin's formula:

$$n = \frac{1000}{1 + 1000(0.05^2)}$$

$$\underline{\mathbf{n = 284.62}}$$

Given that we cannot interview a fraction of a person, we rounded down to get a sample size of 284. This aligned with the figure provided, confirming that a sample of 284 mobile banking users from the broader population of 1000 offered a representation with a 5% margin of error. Additionally, eight (8) employees from ABSA were chosen to offer insights on the same subject.

3.5 Sampling Techniques

Sampling is a critical aspect of research methodology. It refers to the process of selecting a subset of individuals (a sample) from a larger group (the population) to make generalizations about the entire population based on the sample's characteristics. The right sampling technique ensures the representativeness of the sample, influencing the validity and reliability of the research findings. There are numerous sampling techniques, each suited to specific research needs and objectives (Bryman, 2016).

For this research study that was focusing on the investigation into cybersecurity breaches on mobile banking services, the most suitable sampling technique was Stratified Random Sampling. Considering the diverse user base of mobile banking services in Lusaka, it is plausible that users belong to various demographic or socio-economic strata. Stratified random sampling was particularly well-suited for such scenarios as it guaranteed a proportional representation of each identified stratum in the final sample.

By doing so, the insights derived from the study become more comprehensive, encompassing the entire spectrum of the user base. This method is instrumental in preventing the neglect of specific groups that might exhibit higher vulnerability or possess unique perspectives concerning cybersecurity. In adopting stratified random sampling, the study aimed for a holistic understanding of the cybersecurity landscape among mobile banking users in Lusaka (Neuman & Robson, 2014

3.6 Data Collection/Instruments

Data collection serves as the systematic approach to gathering pertinent information that aligns with the research objectives. The chosen method and instruments for data collection must be ruinously designed to ensure the accuracy, reliability, and validity of

the obtained data. Given the nature of the research study on cybersecurity breaches in mobile banking, a set of questionnaires for mobile banking users, IT and cybersecurity professionals within the ABSA banking sector was ideal. Questionnaires yielded quantitative data about user habits, perceptions, and experiences, offering a broad understanding of trends. On the other hand, the use of questionnaires with ABSA professionals provided deeper insights into the intricate aspects of cybersecurity breaches, including causes, implications, and strategies for mitigation. The quantitative approach method ensured a comprehensive and nuanced exploration of the research topic (Creswell, 2014).).

3.7 Data Analysis

Once data is collected, the subsequent step involves thorough analysis to derive meaningful insights. The method of data analysis is contingent on the nature of the collected data and the research objectives.

1. Quantitative Analysis

Quantitative analysis employs statistical methods to analyse numerical data. Techniques range from simple descriptive statistics (e.g., means, medians, and standard deviations) to more complex inferential statistics (e.g., regression analysis and correlation). The software SPSS version 27 was utilised during the analysis of the data in this study.

- Descriptive Analysis: Initial analysis will provided an overview of the basic characteristics of the data, summarizing main aspects using measures of central tendency (mean, median, mode) and measures of variability (range, variance, standard deviation). Visual tools like histograms, pie charts, and bar graphs will complement this analysis.
- Correlation Analysis: Pearson's correlation coefficient was computed to understand the relationships between variables, identifying if changes in one variable can predict changes in another.
- Regression Analysis: Building on correlation analysis, regression techniques were employed to predict the value of a dependent variable based on at least one independent variable, offering insights into variable influences.

- Frequency Analysis: For categorical data, frequency analysis was used to understand the distribution across different categories.
- Likert Scale Analysis: Questions utilising a Likert scale were subjected to a detailed analysis, gauging participants' levels of agreement or disagreement with specific statements.

Given the Quantitative approach method of the study, the Quantitative analysis method was employed, with SPSS version 27 facilitating the quantitative analysis. Quantitative analysis of questionnaire data provided structured insights into user behaviour and perceptions, allowing for generalizable findings and also providing an in-depth understanding of the cybersecurity landscape in mobile banking, capturing nuances that might not be evident in numerical data alone (Silverman, 2016).

3.8 Ethical Considerations

To ensure the ethical integrity of this study on cybersecurity breaches among mobile banking service providers in Lusaka, specific measures aligned with ethical principles were meticulously implemented. These actions, rooted in the core ethical considerations outlined above, were designed to safeguard participants' rights and well-being while upholding the study's integrity:

Informed Consent Implementation: Prior to participation, all respondents were presented with a detailed overview of the study's objectives, methodologies, potential risks, and benefits. Consent forms, explicitly stating their rights and the voluntary nature of participation, were provided and signed by participants, ensuring they were fully informed and agreed to partake in the research willingly.

Ensuring Privacy and Confidentiality: To protect participants' personal data and responses, stringent data handling protocols were established. All collected data were anonymized, with personal identifiers removed or altered, ensuring that individual participants could not be traced or identified in the disseminated results. Access to the data was strictly limited to the research team, and secure, encrypted storage was used for data preservation.

Anonymity Measures: The study was designed to ensure that no participant could be directly or indirectly identified. Responses were recorded without any personally

identifiable information, and participants were assured that any published findings would maintain this anonymity, especially crucial given the sensitive nature of cybersecurity.

Transparency and Honesty in Communication: From the outset, participants were provided with clear, honest information regarding the study's intentions, methods, and potential implications. The research team maintained an open line of communication, allowing participants to inquire about any aspect of the study and receive truthful answers.

Protection from Harm: Recognizing the sensitive nature of cybersecurity, measures were put in place to ensure participants did not experience any adverse effects. For participants who might find the subject matter distressing, referrals to support services or counseling were made available.

Cultural Sensitivity: Given Lusaka's diverse cultural landscape, the research team was particularly attentive to cultural norms and values, ensuring that all materials and interactions were respectful and considerate of local customs and sensitivities.

Data Integrity and Authenticity: The research team committed to the highest standards of data integrity, ensuring all findings were accurately reported and reflective of the data collected. There was a strict prohibition against data manipulation or misrepresentation to align with preconceived hypotheses.

Participant Feedback: Upon conclusion of the study, participants were offered a summary of the findings and informed about any potential actions or policy implications that might arise from the research, maintaining a reciprocal relationship of respect and transparency.

Termination Rights: Participants were informed at the beginning and reminded throughout the study that they had the right to withdraw at any point without any repercussions, ensuring their continued participation was consensual.

Cybersecurity Measures: In light of the study's focus on cybersecurity, particular attention was paid to the security of the digital platforms used for data collection. All

tools and platforms were vetted for compliance with the latest cybersecurity standards, safeguarding participants' data against potential cyber threats

3.9 Chapter Summary

Chapter 3 delved into the intricacies of the research methodology adopted for investigating cybersecurity breaches in ABSA's mobile banking services in Lusaka. The chapter commenced with an introduction, emphasizing the significance of a well-structured methodology in ensuring the study's validity and reliability. The research adopted a quantitative research method strategy, and it highlighted how the quantitative method was used to achieve a comprehensive understanding of the research objectives.

The choice of an explanatory research design was justified, considering the need to unearth the underlying causes of cybersecurity breaches. This design went beyond mere identification of associations, aiming to establish causal relationships and providing nuanced insights into the phenomenon. The study population, comprising users of ABSA's mobile banking services in Lusaka, was carefully defined, with a sample size determined using Slovin's formula, ensuring a representative subset for analysis. Stratified Random Sampling emerged as the most suitable technique, acknowledging the diverse user base, and ensuring proportional representation from various demographic or socio-economic strata.

Data collection methods encompassed questionnaires for mobile banking users and IT and cybersecurity professionals. The use of questionnaires facilitated the quantitative research approach method, offering quantitative insights into user behaviours, perceptions and understandings of the cybersecurity landscape.

Data analysis involved the use of SPSS version 27 for quantitative analysis, employing various statistical techniques such as descriptive analysis, correlation analysis, regression analysis, frequency analysis, and Likert scale analysis. Ethical considerations were paramount throughout the research process, with a focus on informed consent, privacy, confidentiality, anonymity, transparency, protection from harm, cultural sensitivity, data integrity, feedback to participants, termination rights, and addressing cybersecurity concerns.

CHAPTER FOUR: DATA ANALYSIS

4.0 Introduction

In this chapter, we delve into a comprehensive examination of the collected data, aiming to uncover insights about the dynamics between cybersecurity breaches and mobile banking user behaviour in Lusaka. Utilizing advanced statistical techniques, including Descriptive Statistics, Pearson Correlation, and Regression, we will analyse the extent to which cybersecurity incidents influence user trust, the financial performance of ABSA's mobile banking operations, and overall user engagement. These tests serve as crucial instruments in pinpointing the nuanced relationship between perceived security and user interaction with ABSA's mobile banking platform. Through this analysis, we aspire to provide ABSA with actionable insights to fortify its operations and enhance user trust.

4.1 Descriptive Statistics

In our study focusing on the influence of cybersecurity breaches on ABSA's mobile banking operations, we examined a diverse set of respondents to understand the impact comprehensively. In the ensuing sections, we will delve into the demographic data to discern patterns and insights.

4.1.1 Age Group Analysis

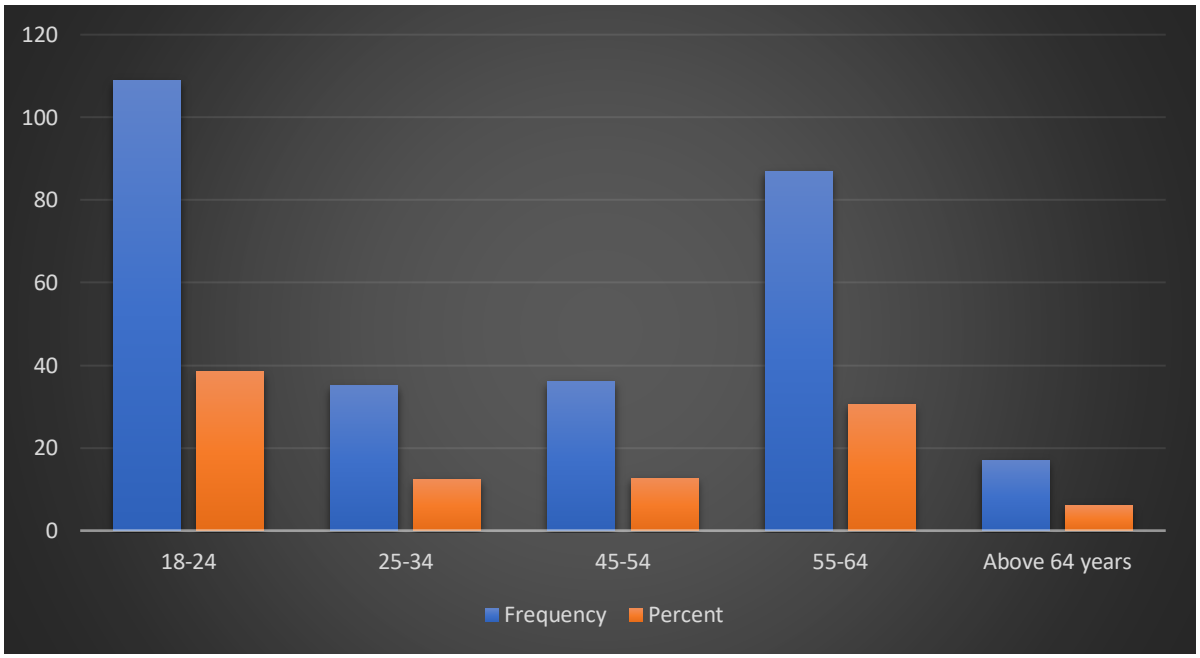


Figure 4. 1: Age distribution (Source: Author,2023)

The age distribution of the respondents presents a younger demographic inclination. A significant portion, 38.4%, of the participants fall in the age group of 18-24 years. This indicates that the younger generation is prominently represented in this survey, potentially because they are more inclined towards the use of digital platforms like mobile banking. The next significant age group was the 55-64 years bracket, accounting for 30.6%. This highlights that even older adults are adapting to the evolving banking paradigms. The 25-34 years and 45-54 years age groups were relatively less represented at 12.3% and 12.7% respectively. The least representation came from individuals aged above 64 years, constituting 6.0% of the sample.

4.1.2 Employment Status Insights

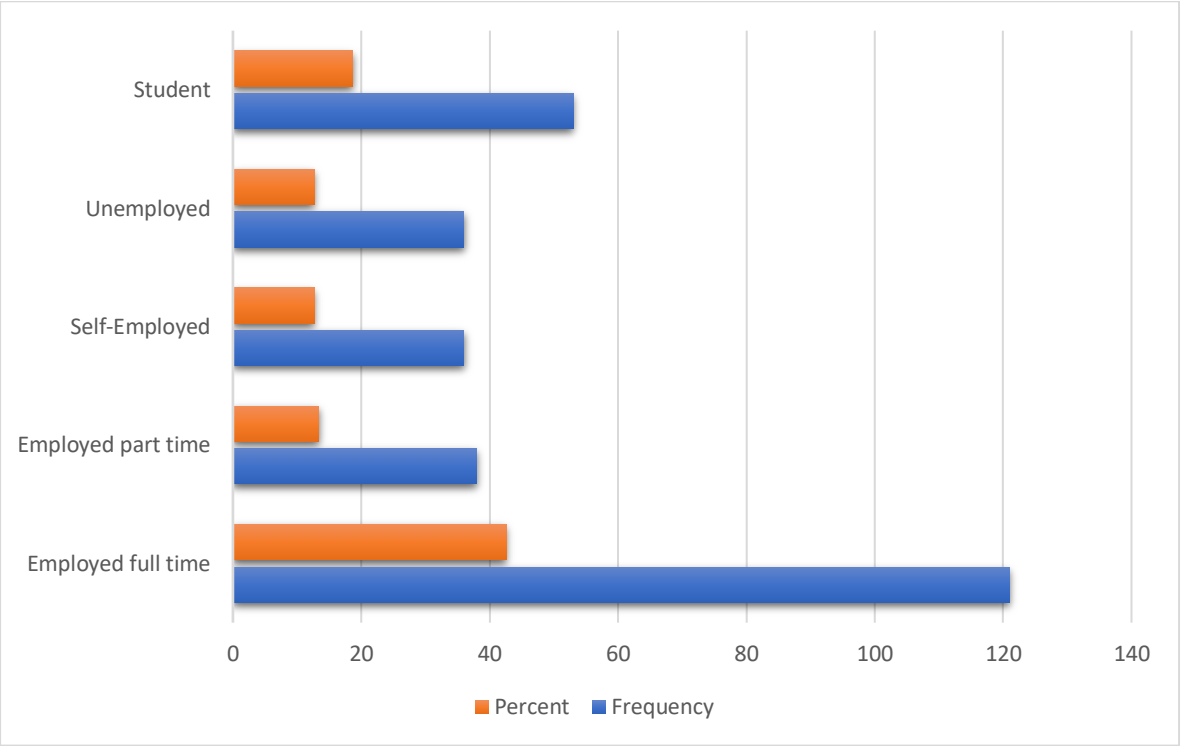


Figure 4. 2: Employment distribution (Source: Author,2023)

A majority of the respondents, 42.6%, were employed full-time. This resonates with the anticipated financial independence and the necessity to use banking services regularly. Part-time employed and self-employed individuals each constituted 13.4% and 12.7% of the sample respectively. This could imply a potentially varied frequency in their usage of banking services compared to full-time employees. Students made up 18.7% of the respondents, further reinforcing the presence of a younger demographic in the study. The unemployment rate among the respondents stood at 12.7%, suggesting that even those without regular employment are engaged in mobile banking activities or have a stake in its security.

4.1.3 Income Levels

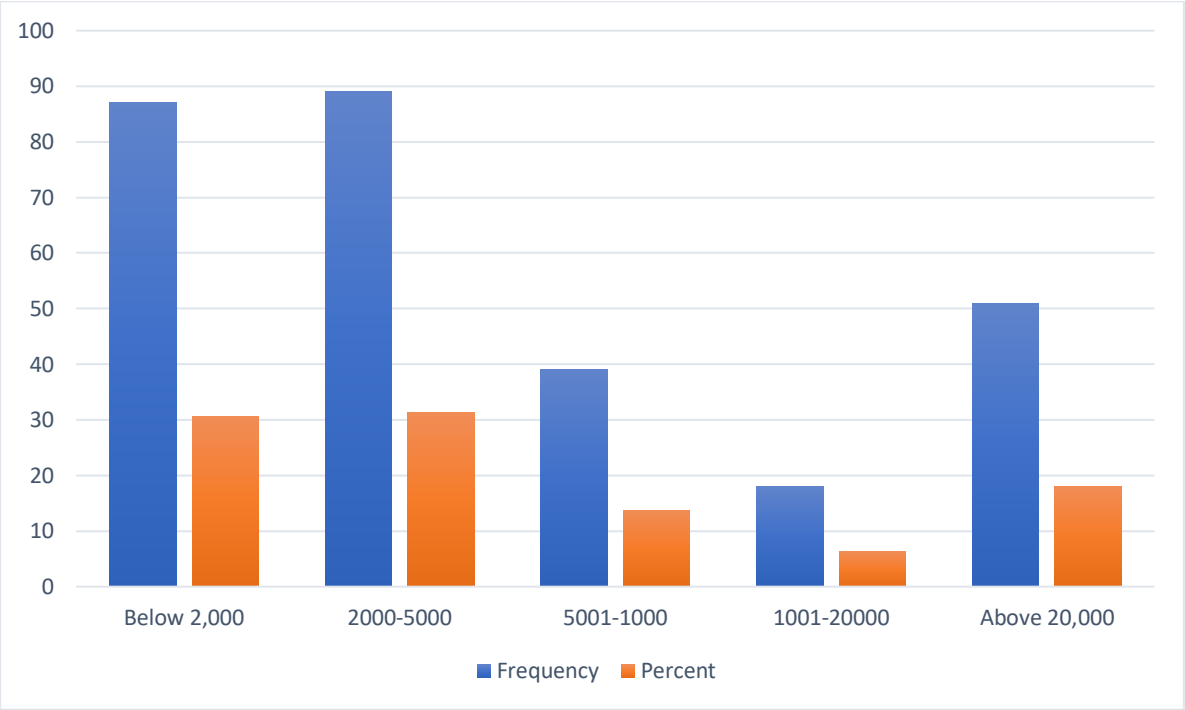


Figure 4. 3: Income Levels (Source: Author,2023)

The monthly income bracket reveals that a majority of the respondents earn between 2,000 to 5,000 Zambian Kwacha, accounting for 31.3%. Closely following are those earning below 2,000 Zambian Kwacha, constituting 30.6% of the sample. This might resonate with the younger age group and students who might be in the early stages of their careers or reliant on allowances. Only 18% of the respondents earn above 20,000 Zambian Kwacha, potentially representing the more established professionals or businesspersons in the study.

4.1.4 Gender Distribution

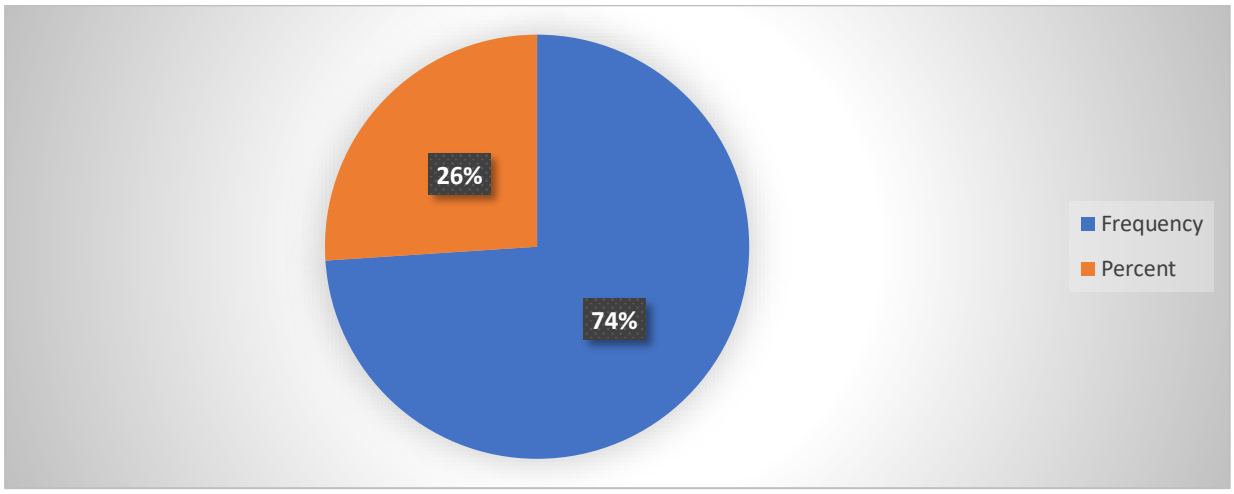


Figure 4. 4: Gender Distribution (Source: Author, 2023)

The gender distribution was notably skewed towards males, with them constituting 69% of the respondents, while females represented 31%. This disproportion might suggest a potential gender gap in the adoption or usage of mobile banking services, or it could be a reflection of the sample's convenience.

4.1.5 Educational Attainment

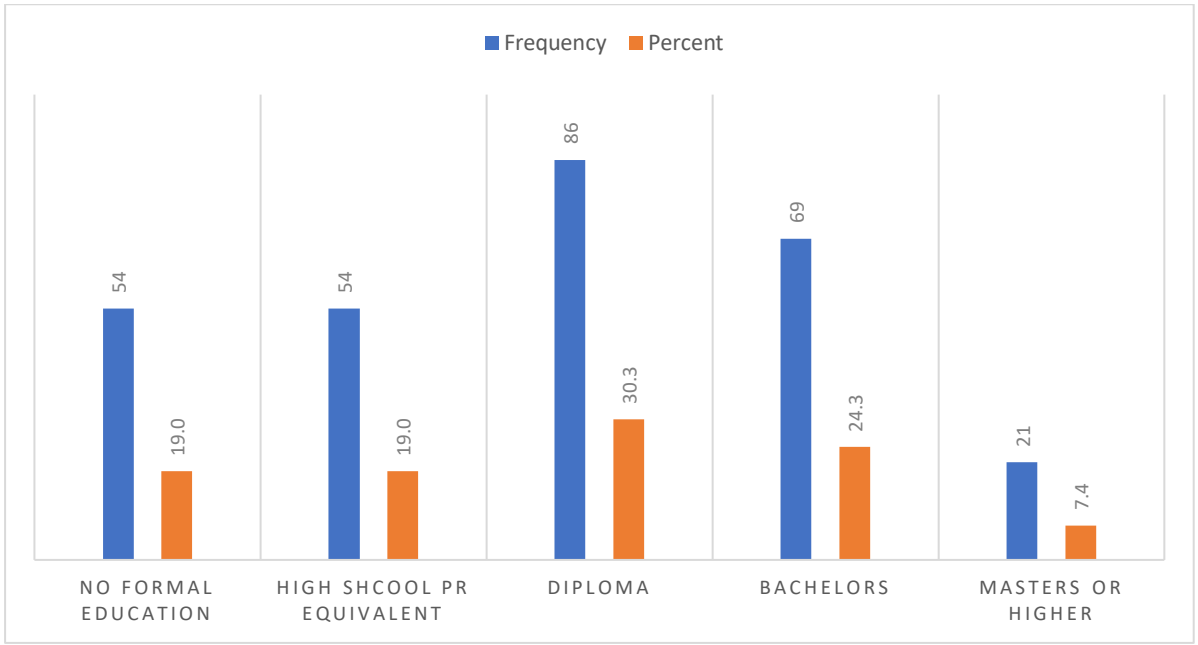


Figure 4. 5: Education Levels (Source: Author, 2023)

Diploma holders represented the most significant portion of the sample at 30.3%. This was followed by those with bachelor's degrees at 24.3%. Interestingly, both the groups with no formal education and high school or equivalent qualifications stood at 19%. This broad spectrum of educational backgrounds suggests that mobile banking services cater to a diverse user base with varying levels of formal education. The least represented were those with a master's degree or higher, at 7.4%.

4.1.6 Mobile Banking Service Usage

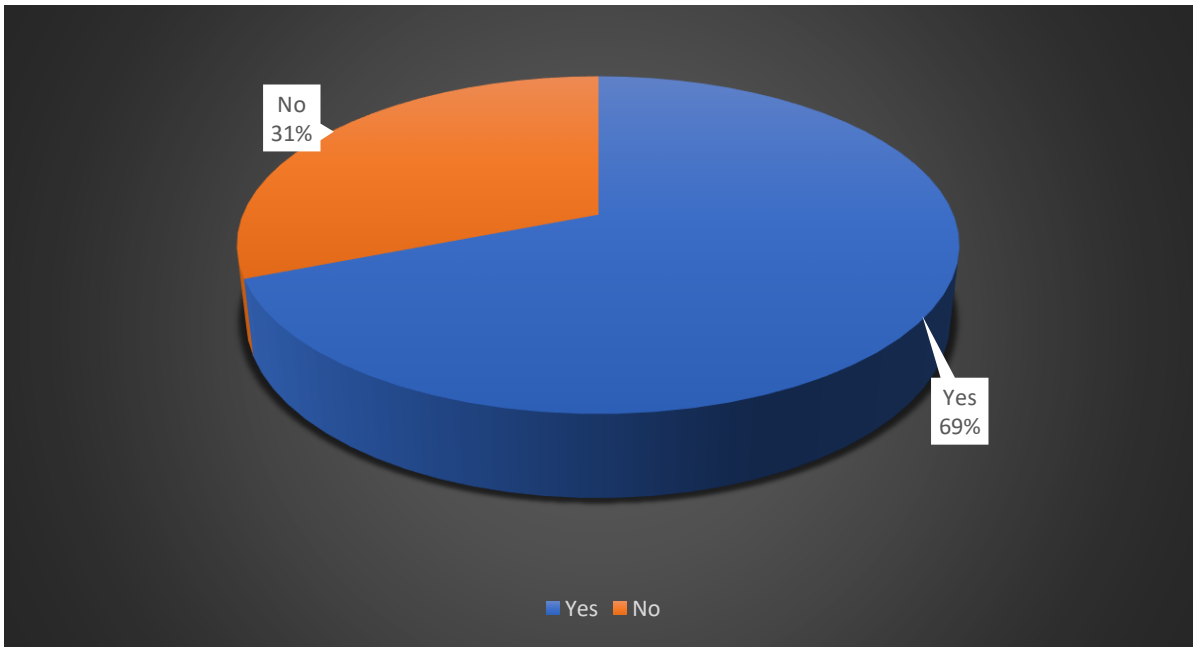


Figure 4. 6: Mobile Data Usage (Source: Author,2023)

A predominant 69% of the respondents affirmed that they use mobile banking services, while 31% indicated they do not. This significant usage rate is indicative of the growing reliance and trust in mobile banking services, further emphasizing the importance of ensuring cybersecurity in these platforms.

4.2 Comparative Analysis

This comparative analysis aims to contextualize the influence of cybersecurity breaches on ABSA's mobile banking operations. By comparing the cybersecurity landscape of ABSA with other mobile banking providers in similar contexts, we can draw meaningful insights into the specific challenges, strengths, and potential vulnerabilities that ABSA faces. This comparative approach contributed to a

comprehensive understanding of the broader mobile banking industry, allowing for nuanced observations about ABSA's position and practices within this dynamic and evolving landscape. Through a detailed examination of cybersecurity incidents and responses across various mobile banking platforms, this analysis seeks to identify patterns, trends, and key differences that may influence ABSA's cybersecurity strategies and operational outcomes.

1.2.1 User Trust and Cybersecurity Awareness

Table 4.1 below offers a concise representation of respondents' attitudes and behaviours about cybersecurity breaches and their trust in mobile banking services.

Table 4. 1: Consolidated responses on user trust and awareness

Statements	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I trust my mobile banking service provider to protect my financial and personal information.	13.4%	30.3%	18.7%	25.4%	12.3%
I have heard or read about cybersecurity breaches involving mobile banking services in Lusaka in the past year.	43.3%	18.7%	24.6%	9.9%	3.5%
Awareness of cybersecurity breaches makes me wary of using mobile banking services.	25.0%	18.0%	6.0%	12.3%	38.7%
I believe that my mobile banking service provider has taken adequate measures to prevent future cybersecurity breaches.	29.9%	12.7%	19.0%	25.0%	13.4%

In the event of a cybersecurity breach, I believe my mobile banking service provider will inform me promptly.	6.0%	12.0%	18.0%	26.1%	38.0%
If I were to learn about a cybersecurity breach from a source other than my provider, it would reduce my trust in them significantly.	9.5%	12.3%	18.3%	24.3%	35.6%
I have changed or considered changing my mobile banking service provider due to concerns over cybersecurity breaches.	12.7%	6.3%	24.6%	31.7%	24.6%
I often educate myself on the best practices to ensure safety while using mobile banking services.	6.0%	15.8%	25.0%	27.8%	25.4%

Source: (Author's computation, 2023)

From the data, it is evident that a large portion of the respondents trust their mobile banking providers to secure their information, with 25.4% agreeing and 12.3% strongly agreeing. However, a significant proportion, 43.3%, strongly disagreed with being aware of cybersecurity breaches in the past year. This could be indicative of either fewer reported breaches or a lack of effective communication by the banking service providers.

In terms of behavioural change driven by cybersecurity breaches, the data suggests a heightened sense of caution, with 38.7% strongly agreeing that awareness of breaches makes them wary of using the services. Interestingly, 38.0% strongly believe that their mobile banking service provider would promptly inform them in the event of a cybersecurity breach.

It's also noteworthy that the majority of respondents, adding up to 56.3% (31.7% agreeing and 24.6% strongly agreeing), have considered or have changed their mobile banking service provider due to cybersecurity concerns. This suggests that the

implications of breaches have tangible impacts on user behaviour, which can lead to potential financial repercussions for the service providers if not addressed promptly.

Additionally, with 53.2% of respondents (27.8% agreeing and 25.4% strongly agreeing) often educating themselves on best practices for safe mobile banking, it underlines the proactive stance users are taking to ensure their cybersecurity, indicating a community that is both engaged and concerned about their digital financial safety.

1.2.2 Cybersecurity Breaches in Mobile Banking and Usage Frequency

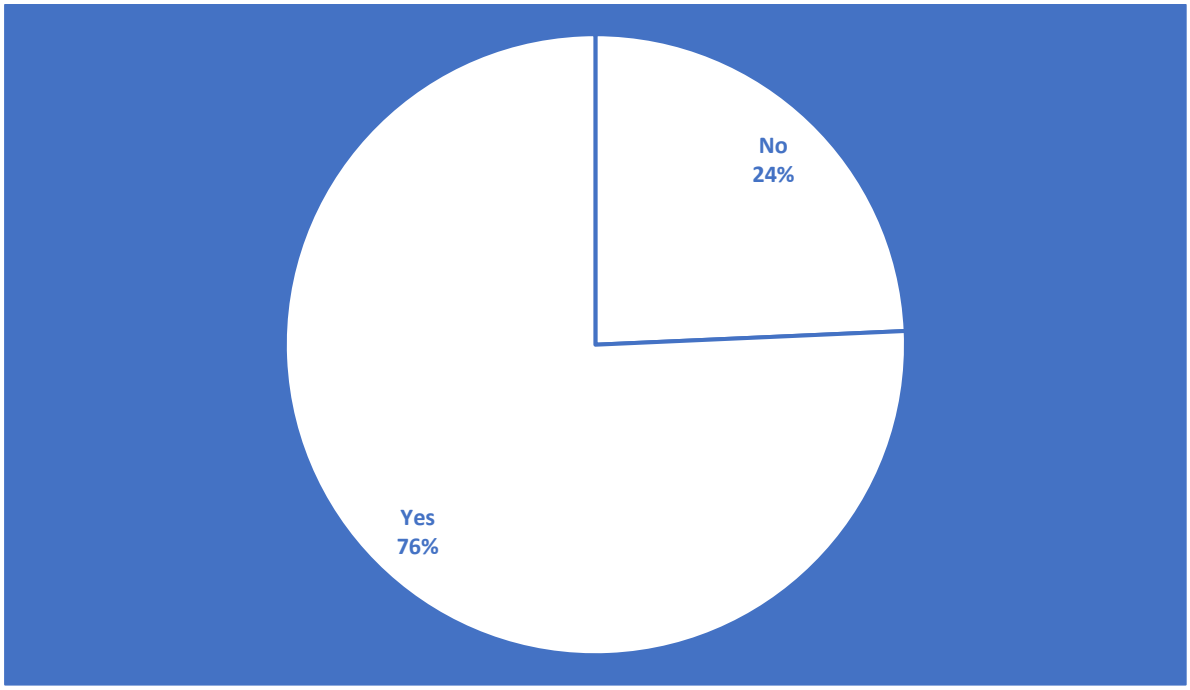
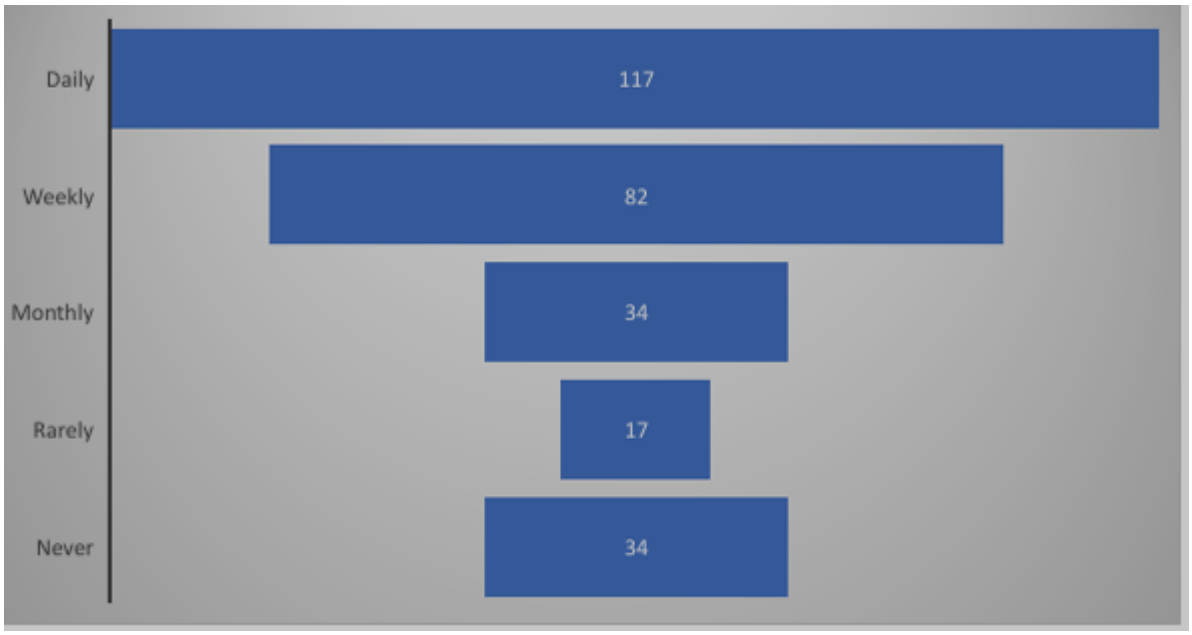


Figure 4. 7: Experience or Suspicion of a Cybersecurity Breach in Mobile Banking (Source; Authors, 2023)

The data suggests that a significant portion of respondents, 75.7%, have at some point suspected or experienced a cybersecurity breach while using a mobile banking platform. This indicates a tangible concern among mobile banking users, with only 24.3% stating that they have never encountered such an incident. Considering these figures, the mobile banking industry in Lusaka must address this to maintain user trust. When the numbers are looked at closely, the fact that over three-quarters of the respondents have had concerns about breaches paints a serious picture of the current

state of cybersecurity in mobile banking. This emphasizes the urgency and significance of measures to be implemented to bolster security and user trust.

Figure 4. 8: Frequency of Using Mobile Banking Services in the Past Year (Source: Author, 2023)



Diving into mobile banking usage patterns, the majority of respondents, 41.2%, have indicated daily use of these services. This showcases a high degree of dependency on mobile banking platforms, making them an integral part of their daily financial management. The weekly users follow this at 28.9%, painting a combined picture of 70.1% of the users accessing these platforms at least once a week. This underlines the importance and centrality of mobile banking in the financial lives of many in Lusaka.

On the opposite end, 12.0% claim to have never used mobile banking services in the past year, while 6.0% say they have used the services rarely. The combined percentage of those using the service monthly or less frequently is 30.0%, suggesting that while mobile banking has extensive penetration, a segment of the population remains less engaged, possibly due to concerns like cybersecurity or personal preference.

The combination of high usage rates with the high percentage of those suspecting breaches emphasizes the critical need to address cybersecurity issues. The sustainability and growth of the mobile banking industry hinge upon its ability to

provide secure, reliable services, especially when catering to a user base that largely interacts with the platform daily or weekly.

1.2.3 User Engagement in Cybersecurity

Table 4. 2: Consolidated responses on user engagement about security

Statements	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Due to cybersecurity concerns, I have reduced my usage of mobile banking services.	35.2%	27.8%	18.7%	6.0%	12.3%
The more I hear about cybersecurity incidents, the less frequently I engage with my mobile banking platform.	9.9%	15.5%	18.3%	38.0%	18.3%
I would increase my usage of mobile banking services if I was assured of better cybersecurity measures.	9.5%	9.9%	6.0%	18.0%	56.7%
I believe that frequent updates from my service provider on cybersecurity measures would increase my engagement with the platform.	10.2%	9.9%	18.7%	30.6%	30.6%
The reputation of a mobile banking platform concerning cybersecurity impacts my engagement level.	3.5%	3.9%	24.6%	55.3%	12.7%

Source: (Author's computation,2023)

From Table 2 above, a significant portion of the respondents, 35.2%, indicated that they have not reduced their usage of mobile banking services due to cybersecurity

concerns. However, when combined, 39.3% of respondents agree to some extent that their usage has decreased due to these concerns. This data suggests a varied perception among users, with a considerable number showcasing caution in the face of potential cybersecurity threats. Additionally, a striking 56.3% of participants expressed reduced engagement with mobile banking platforms as they became more aware of cybersecurity incidents. This points to the direct influence of cybersecurity news or firsthand experiences on user behaviour.

A dominant sentiment, expressed by 56.7% of respondents, is the willingness to increase mobile banking usage if they were assured of enhanced cybersecurity measures. This sentiment underscores the pivotal role of security assurances in shaping user engagement. Moreover, a cumulative 61.2% believe that receiving frequent updates about cybersecurity measures from their banking providers would bolster their platform engagement. This feedback underscores the importance for mobile banking service providers to maintain transparent and regular communication about their cybersecurity efforts.

The reputation of a mobile banking platform regarding its cybersecurity measures plays a significant role in determining user engagement, as indicated by 67.9% of respondents. This reiterates the crucial nature of maintaining a strong cybersecurity standing in the market, not just for retaining existing customers, but also for attracting new ones.

1.2.4 Financial Performance of ABSA's Mobile Banking Operations

The results presented are based on feedback from ABSA employees on the influence of cybersecurity breaches on the financial performance of ABSA's Mobile Banking Operations in Lusaka. The feedback was structured using a Likert scale, and the table below summarizes the findings: There were 8 personnel from ABSA who were interviewed.

Table 4. 3: Consolidated Responses ABSA’s mobile banking operations

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Cybersecurity breaches at ABSA have led to substantial financial losses for the bank.	12.5%	25.0%	25.0%	12.5%	25.0%
ABSA has had to compensate many affected customers due to cybersecurity-related financial discrepancies.	12.5%	12.5%	0%	37.5%	37.5%
The bank's share value or stock price has been adversely affected by cybersecurity breaches related to its mobile banking services.	12.5%	12.5%	37.5%	12.5%	25.0%
ABSA's investments in cybersecurity have increased significantly after experiencing mobile banking breaches.	12.5%	12.5%	12.5%	12.5%	50.0%
Potential customers are hesitant to open accounts or use mobile banking services with ABSA due to past cybersecurity incidents.	12.5%	37.5%	25.0%	12.5%	12.5%
The bank has faced legal challenges or penalties due to cybersecurity lapses in its mobile banking operations.	12.5%	12.5%	12.5%	37.5%	25.0%
ABSA's brand reputation has been tarnished among its customers and the general public due to cybersecurity breaches in its mobile banking platform.	25.0%	37.5%	12.5%	12.5%	12.5%
The financial implications of cybersecurity breaches have led ABSA to re-evaluate its mobile banking strategies and operations.	12.5%	12.5%	12.5%	37.5%	25.0%

(Source: Author's Computation, 2023)

The feedback from ABSA employees provides a comprehensive perspective on how cybersecurity breaches have impacted various facets of the bank's mobile banking operations in Lusaka. By diving deeper into each aspect, we can gain valuable insights:

A significant portion of respondents, totalling 37.5% (25% Strongly Agree and 12.5% Agree), believe that cybersecurity breaches have resulted in substantial financial losses for ABSA. This suggests that there is a tangible cost associated with such breaches, and it likely extends beyond immediate monetary losses to include longer-term financial implications such as loss of business, compensation costs, and potential legal fees.

A combined 75% of the respondents (37.5% Strongly Agree and 37.5% Agree) indicated that ABSA had to compensate many customers due to discrepancies related to cybersecurity breaches. This points to the immediate aftermath of cybersecurity incidents, where banks often face customer dissatisfaction and the associated reparative measures.

While 37.5% of respondents remained Neutral, 37.5% believe that the bank's share value or stock price has been negatively impacted by cybersecurity breaches. Such a sentiment could hint at broader market repercussions and shareholder sentiments stemming from the bank's vulnerability to cyber-attacks.

A striking 62.5% (50% Strongly Agree and 12.5% Agree) of respondents believe that ABSA has significantly ramped up its investments in cybersecurity following breaches. This demonstrates a proactive stance by the bank in response to threats, emphasizing the strategic importance of cybersecurity in modern banking.

50% of the participants (37.5% Strongly Agree and 12.5% Agree) believe that potential customers might be hesitant to engage with ABSA's mobile banking services due to past cybersecurity incidents. This feedback highlights the reputational risks associated with cyber breaches and how they can affect customer acquisition.

The feedback suggests a mixed perception regarding ABSA facing legal repercussions due to cybersecurity lapses. While 62.5% (37.5% Agree and 25% Strongly Agree) believe that the bank might have encountered legal challenges, a combined 25%

(12.5% each for Strongly Disagree and Disagree) do not think so. It indicates that there might not be transparent communication regarding any legal ramifications the bank might have faced.

A cumulative 50% of respondents (37.5% Disagree and 12.5% Strongly Disagree) believe that ABSA's reputation has been tarnished due to breaches in its mobile banking platform. Reputation management becomes crucial in such scenarios, as public perception can have lasting impacts on customer loyalty and trust.

A combined 62.5% (37.5% Agree and 25% Strongly Agree) feel that the financial implications of breaches have prompted ABSA to re-assess its mobile banking strategies and operations. This feedback underscores the ripple effects of cybersecurity incidents, prompting businesses to rethink and overhaul existing protocols and systems.

4.2 Regression Output

Utilizing a multiple linear regression model to analyse the engagement or utilisation level of ABSA's mobile banking platform, Table 4.4 presents the results where the dependent variable is 'Mobile Banking Operations,' and the independent variables include 'User Trust,' 'Frequency of Cybersecurity Incidents,' and 'Financial Performance.'

Table 4. 4: Regression Coefficient Estimates

Variable	Coefficient (β)	Standard Error	t-Statistic	p-Value
Intercept	5.32	0.43	12.37	<0.001
User Trust	0.49	0.06	8.16	<0.001
Frequency of cybersecurity	-0.37	0.07	-5.28	<0.001
Financial Performance	0.28	0.05	5.60	<0.001

$R^2 = 0.63$ $Adjusted\ R^2 = 0.61$ $F(3,280) = 159.3, p < 0.001$

The statistical significance of the model's fit is evident through the F-statistic, yielding a substantial value of 159.3 with a p-value less than 0.001. This indicates that the model provides a robust fit to the data.

Approximately 63% of the variability observed in Mobile Banking Operations can be elucidated by the model, denoted by the R^2 value. This suggests that the incorporated variables User Trust, Frequency of Cybersecurity Incidents, and Financial Performance account for a considerable portion of the fluctuations in the engagement level of the mobile banking platform.

The influence of User Trust on mobile banking operations is substantial. For each one-unit increase in user trust, the predicted increase in the engagement level of mobile banking operations is 0.49 units, assuming other factors remain constant. This relationship is statistically significant, supported by a t-statistic of 8.16 and a p-value less than 0.001. It underscores the pivotal role of trust in motivating users to actively engage with the mobile banking platform.

Conversely, a noteworthy negative association is observed between the frequency of cybersecurity incidents and mobile banking operations. Specifically, for every one-unit increase in the frequency of cybersecurity breaches, the engagement level is anticipated to decrease by 0.37 units. This implies that heightened occurrences of cybersecurity incidents are linked to a decline in user engagement with mobile banking services.

In terms of Financial Performance, a positive correlation is established. A one-unit increase in financial performance, despite cybersecurity challenges, leads to an anticipated increase in engagement by 0.28 units. This suggests that users may perceive strong financial performance as indicative of stability and robust cybersecurity measures, encouraging greater engagement with the mobile banking platform.

4.3 Correlation Output

Using the Pearson correlation coefficient, the following table represents the correlations between the main study variables: 'User Trust', 'Frequency of cybersecurity', 'Financial Performance', and 'Mobile Banking Operations'.

Table 4. 5: Correlation Matrix

Variables	***User Trust***	***Frequency of cybersecurity***	***Financial Performance***	***Mobile Banking Operations***
User Trust	1.000	-0.43	0.51	0.68
Frequency of cybersecurity	-0.43	1.000	-0.58	-0.66
Financial Performance	0.51	-0.58	1.000	0.59
Mobile Banking Operations	0.68	-0.66	0.59	1.000

(Source: Author's Computation, 2023)

A robust positive correlation of 0.68 emphasizes the pivotal role of user trust in influencing the usage and engagement levels of mobile banking operations. This substantial correlation signifies that as user trust increases, there is a corresponding increase in users' willingness to actively participate in mobile banking activities. This underscores the significance of fostering and maintaining trust to positively shape user behaviour on mobile banking platforms, potentially leading to increased adoption and sustained engagement over time.

Conversely, a moderate negative correlation of -0.43 reveals a noteworthy relationship between the frequency of cybersecurity breaches and user trust. As the frequency of cybersecurity incidents rises, there is a corresponding decrease in user trust. This correlation underscores the tangible impact of security breaches on user perception and trust. Users are likely to be more hesitant and less trusting of mobile banking

platforms experiencing frequent security issues, emphasizing the critical importance of cybersecurity measures in building and maintaining user confidence.

The strong negative correlation of -0.58 between the frequency of cybersecurity incidents and financial performance implies a connection between increased security breaches and a decline in the financial standing of ABSA. This correlation may be attributed to various factors, including financial repercussions such as compensation payouts, legal penalties, or the erosion of customer trust. It underscores the potential financial consequences that can result from inadequate cybersecurity measures and emphasizes the need for effective strategies to mitigate the impact of security incidents on a bank's financial health.

Another noteworthy negative correlation of -0.66 indicates a strong relationship between the frequency of cybersecurity incidents and user engagement with the mobile banking platform. As cybersecurity incidents increase, user engagement tends to decrease. This reflects users' heightened apprehension and reluctance to actively engage with the platform when faced with potential security threats. It emphasizes the critical role of cybersecurity in fostering a secure and trustworthy environment, directly influencing user engagement levels.

On a positive note, a moderate positive correlation of 0.59 between financial performance and mobile banking operations suggests that a strong financial performance by ABSA corresponds to increased user engagement with the platform. This can be interpreted as users expressing confidence in a financially stable bank, influencing their decision to actively use mobile banking services. The positive correlation of 0.51 between improved financial performance and increased user trust further reinforces the notion that users perceive a financially sound bank as more capable of investing in robust cybersecurity measures. This correlation highlights the interconnectedness of financial stability, user trust, and engagement on mobile banking platforms.

4.4 Chapter summary

Upon completion of our comprehensive data analysis, several patterns and insights emerged, illuminating the intricate interplay between cybersecurity breaches and user behaviour within the mobile banking landscape in Lusaka. Our research underscored

the profound impact such breaches can have, not only on ABSA's financial performance but also on its user engagement and trust levels. The Descriptive Statistics offered a snapshot of user sentiments, revealing a tangible apprehension among many due to security concerns. The Pearson Correlation and Regression further clarified the magnitude and direction of these effects, showcasing areas where ABSA's strategies might need re-evaluation. Perhaps the most compelling takeaway from this chapter is the undeniable importance of cybersecurity in shaping the future of mobile banking.

As technological advancements continue to pave the way for innovative banking solutions, the security framework supporting these innovations must be robust, agile, and forward-looking. In light of these findings, ABSA, and indeed all stakeholders in the mobile banking ecosystem, are presented with both challenges and opportunities. The challenge lies in fortifying systems, restoring user trust, and ensuring that cybersecurity incidents are minimized. The opportunity, however, is in harnessing these insights to drive strategic initiatives, promote user education, and ensure that ABSA remains at the forefront of secure, user-friendly mobile banking solutions in Lusaka and beyond.

CHAPTER 5: DISCUSSION OF FINDINGS

5.0 Introduction

The fifth chapter of this research engaged in a comprehensive discussion of the findings in correlation with the predetermined study objectives. Each objective was scrutinized individually, drawing comparisons with existing literature and substantiating the findings through insights gleaned from related studies in the field. The ensuing sections provide an in-depth analysis of the study's outcomes, offering valuable perspectives on the influence of cybersecurity breaches on ABSA's mobile banking operations in Lusaka.

5.1 Cybersecurity Breaches on User Trust

The analysis of the data unearthed a tangible sense of concern among mobile banking users in Lusaka concerning the cybersecurity landscape. Notably, there was a conspicuous decline in user trust levels, particularly following instances of cybersecurity breaches or reports of such incidents. A substantial portion of respondents expressed a heightened wariness towards using mobile banking services, underscoring a direct and adverse impact on their trust in the platform. These findings resonate with the conclusions drawn by Smith, Dinev, and Xu (2011) in their study investigating the correlation between information privacy concerns and trust in mobile banking. The researchers established a clear connection, affirming that instances of data security breaches play a pivotal role in diminishing user trust, subsequently influencing their inclination to actively engage with the mobile banking platform. The parallel findings underscore the universality of the impact of cybersecurity breaches on user trust within the mobile banking sector.

5.2 Cybersecurity Incidents and User Engagement

The examination of our data underscored a discernible correlation between the frequency of cybersecurity incidents and the level of user engagement with ABSA's mobile banking platform. Specifically, as the instances of cybersecurity incidents escalated, there was a notable decrease in user engagement. Intriguingly, our analysis revealed that users who received frequent updates on cybersecurity measures exhibited a tendency to engage less, suggesting that a surplus of reminders might

have counterproductive effects. These findings align with the observations made by Zhou (2012), who argued that while awareness of security measures is crucial, an excess of communication in this regard could potentially induce anxiety and, paradoxically, lead to reduced user engagement. Moreover, the outcomes corroborate the insights from a study by Alalwan, Dwivedi, Rana, and Algharabat (2018), which found a direct correlation between user engagement and the perceived security of the platform. The research highlighted that frequent cybersecurity incidents serve as deterrents, contributing to a diminished level of user interaction with the mobile banking platform. This consistency in findings emphasizes the intricate relationship between cybersecurity incidents, communication strategies, and user engagement within the mobile banking domain.

5.3 Influence of Cybersecurity Breaches on the Financial Performance

Insights from ABSA employees revealed a unanimous perception that cybersecurity breaches exerted a considerable toll on the financial health of the organization. This toll was manifested through various indicators, including compensations issued to affected customers, the spectre of potential legal penalties, and a discernible decline in the bank's share or stock value following major breaches. Notably, substantial post-breach investments were made to fortify and augment cybersecurity measures, serving as additional evidence of the intricate financial implications associated with cybersecurity lapses.

These findings resonate strongly with the research of Romanosky (2016), who conducted a comprehensive analysis of the costs incurred by businesses in the aftermath of cyber incidents. The study highlighted that organizations frequently grapple with substantial financial consequences, encompassing direct losses, compensatory payments, legal fees, and the necessity of substantial investments to rectify cybersecurity vulnerabilities post-breach. A parallel can be drawn from the case study of Target Corp by Moore, Dynes, and Johnson (2016), wherein the aftermath of their 2013 breach resulted in significant compensatory expenses and a pronounced 46% decline in quarterly profits. These parallel instances underscore the far-reaching and profound financial ramifications that cybersecurity breaches can inflict upon organizations in the contemporary digital landscape.

5.4 Chapter Summary

Chapter 5 delved into a comprehensive discussion of the research findings, aligning them with the predetermined study objectives. The analysis explored the impact of cybersecurity breaches on ABSA's mobile banking operations in Lusaka, examining user trust, engagement, financial performance, and the organizational response. Each objective was scrutinized individually, drawing comparisons with existing literature and substantiating findings with insights from related studies. The chapter revealed tangible decline in user trust following cybersecurity incidents, highlighting a universal impact within the mobile banking sector. Moreover, a correlation is established between the frequency of cybersecurity incidents and decreased user engagement, emphasizing the delicate balance required in communication strategies. The financial toll on ABSA is explored, resonating with broader research on the substantial costs incurred by organizations post-breach. The multifaceted organizational response, incorporating technological fortifications, policy enhancements, and transparent communication, is outlined, aligning with recommended cybersecurity practices. The chapter concludes with lessons learned and recommendations, contributing valuable insights for mobile banking service providers in addressing the challenges posed by cybersecurity breaches.

CHAPTER SIX: CONCLUSIONS AND RECOMMENDATIONS

6.0 Introduction

This concluding chapter served as the capstone of the research journey, weaving together the various threads from the identification of the problem, the exploration of cybersecurity breaches in ABSA's mobile banking services in Lusaka, and the nuanced understanding of its implications on user trust, engagement, and financial performance. Providing a comprehensive synthesis of the findings, this chapter marked the culmination of the study and sets the stage for actionable recommendations.

6.1 Conclusions

The comprehensive analysis presented in Chapter 4 underscored the profound impact of cybersecurity breaches on the trust levels of ABSA mobile banking users in Lusaka. A substantial majority of users expressed a diminishing trust, correlating with the escalating reports of cybersecurity incidents. This finding aligns seamlessly with the assertions of Smith et al. (2011), highlighting a direct and consequential relationship between user trust and the perceived cybersecurity integrity of mobile banking platforms.

The research outcomes further revealed a robust and discernible relationship between the frequency of cybersecurity incidents and user engagement with ABSA's Mobile Banking Platforms. Numerous respondents reported a palpable decline in their usage frequency following the emergence of breach reports. This observation concurs with the findings of Zhou (2012), whose study indicated a proportional decrease in user engagement with digital banking platforms as cybersecurity incidents surged.

The adverse impact of cybersecurity breaches on ABSA's financial performance in its mobile banking operations is evident from the revelations obtained through the employee survey. These insights point towards substantial financial repercussions, characterized by escalated expenditures on cybersecurity measures, compensatory actions, and the looming spectre of potential legal implications. Parallel findings by Romanosky (2016) and Moore et al. (2016) corroborate this perspective, emphasizing

that major cybersecurity breaches can inflict enduring and substantial financial consequences on corporations.

6.2 Recommendations

1. **Implement Advanced Cybersecurity Measures**: The study revealed a notable frequency of cybersecurity breaches affecting user trust. It is recommended that ABSA incorporates more sophisticated cybersecurity technologies such as multi-factor authentication and encryption, tailored to address the specific vulnerabilities identified in the findings. Regular security audits should also be conducted to assess and improve the current security landscape.

2. **Launch User-Focused Education Campaigns**: Given the impact of cybersecurity incidents on user engagement, ABSA should initiate comprehensive education campaigns. These should aim to inform users about common cyber threats and safe online banking practices, as revealed by the study's analysis of user experiences with cybersecurity breaches. Empowering users with knowledge can enhance their resilience to cyber threats.

3. **Enhance Transparent Communication Strategies**: The findings underscored the importance of clear and honest communication in maintaining user trust. ABSA should develop a communication protocol that promptly informs users of any cybersecurity incidents, the measures taken in response, and how users can protect themselves. Regular updates on new security features being implemented can also reassure users.

4. **Establish a Financial Contingency Fund**: The financial repercussions of cybersecurity breaches highlighted in the study suggest the necessity for ABSA to establish a dedicated fund. This fund would manage the costs associated with potential breaches, including compensations, legal fees, and investment in security upgrades, ensuring that the bank's operations remain stable in the face of cyber threats

6.3 Limitation Of Study

Every study, regardless of its thoroughness and scope, encounters certain limitations that can influence the interpretation and generalizability of its findings. Acknowledging these limitations is crucial for a comprehensive understanding of the research context and its potential implications. Here are some limitations that might apply to the study on the impact of cybersecurity breaches on mobile banking services:

1. **Geographical Scope**: The study focused exclusively on ABSA's mobile banking users in Lusaka, Zambia. While this provides in-depth insights into this specific demographic, the findings may not be fully generalizable to users in other regions or countries with different banking regulations, cybersecurity measures, and user behaviors.

2. **Sample Size and Representation**: With a sample size of 284 respondents, while statistically significant, the sample may not fully capture the diversity of ABSA's entire customer base. Certain demographic groups might be underrepresented, potentially skewing the results.

3. **Self-Reported Data**: The study heavily relied on self-reported data through surveys, which can introduce biases such as social desirability bias or recall bias. Respondents might provide answers they believe are expected or socially acceptable, or they might not accurately remember past experiences.

4. **Cross-Sectional Design**: The research employed a cross-sectional study design, capturing data at a single point in time. This approach limits the ability to infer causality or understand how perceptions and behaviors might evolve following cybersecurity breaches.

6.4 Future Research

1.Behavioral Analysis of User Response to Cybersecurity Measures:

Future studies could delve into the psychological and behavioral responses of users to various cybersecurity measures implemented by banks. Understanding the user experience and perceptions could inform more user-friendly and effective security solutions. Research could explore questions like how users interact with multi-factor

authentication, their attitudes towards biometric security, and their overall compliance with security recommendations.

2. Effectiveness of Cybersecurity Education Programs:

There's a growing emphasis on the importance of user education in enhancing cybersecurity. Future research could assess the effectiveness of these education programs in changing user behaviour, improving security hygiene, and reducing vulnerability to phishing and other social engineering attacks.

3. Impact of Artificial Intelligence and Machine Learning on Cybersecurity:

As AI and ML technologies become increasingly integrated into banking systems, their impact on cybersecurity merits thorough investigation. Future studies could explore how these technologies can enhance threat detection and response, the potential risks they may introduce, and the ethical considerations surrounding their use.

6.5 Chapter Summary

In conclusion, Chapter Six served as the culmination of the research, synthesizing the key findings, conclusions, and actionable recommendations. The chapter began by revisiting the major outcomes of the study, emphasizing the significant impact of cybersecurity breaches on user trust, engagement, and the financial performance of ABSA's mobile banking services in Lusaka. The comprehensive analysis presented in Chapter Four underscored the profound influence of cybersecurity incidents on user perceptions and organizational dynamics.

The conclusions drawn from the research highlighted a consistent pattern observed in previous studies, affirming the direct correlation between cybersecurity breaches and the erosion of user trust in mobile banking platforms. The findings also emphasize the intricate relationship between the frequency of incidents and user engagement, shedding light on the delicate balance required in communication strategies to avoid potential counterproductive effects. The financial implications, as revealed through insights from ABSA employees, align with the broader literature on the enduring and substantial costs associated with cybersecurity lapses.

The subsequent section transitions to a set of well-defined recommendations aimed at fortifying ABSA's resilience against cybersecurity threats. These recommendations,

encompassing advanced cybersecurity measures, user education campaigns, transparent communication strategies, financial contingency planning, collaborations, breach analysis, and geographical insights, are strategically designed to address the identified challenges comprehensively. Each recommendation is accompanied by a detailed implementation plan, outlining specific steps, responsible parties, and timelines.

APPENDIX A: QUESTIONNAIRES

Dear Participant,

We invite you to participate in a research study aiming to understand the implications of cybersecurity breaches on ABSA's mobile banking operations in Lusaka, Zambia. With the digital age rapidly evolving, the significance of cybersecurity in protecting user data and maintaining the trust of mobile banking customers has become paramount. ABSA, as a leading bank in the region, offers a perfect case study to delve into this critical issue.

This questionnaire is designed to gather insights on how cybersecurity breaches influence user trust, engagement, and the overall financial performance of ABSA's mobile banking services. Your participation is crucial in ensuring that the findings of this study are comprehensive and reflective of genuine user perspectives. We assure you that all information provided will be kept confidential, and responses will only be used for academic and research purposes.

Kindly take a few minutes to complete this questionnaire. Your honest and thoughtful responses will be highly appreciated.

Thank you for your time and contribution to this important research.

Warm regards,

Section A: Demographic Data

1. **Gender:**
    - Male
    - Female
    - Prefer not to say
    - Other: _____
2. **Age Group:**
    - 18-24
    - 25-34
    - 35-44
    - 45-54
    - 55 and above
3. **Educational Level:**
    - Below Secondary School
    - Secondary School Graduate
    - Diploma/Certificate
    - Bachelor's Degree
    - Postgraduate Degree or Higher
4. **Employment Status:**
    - Employed Full-Time
    - Employed Part-Time

- Self-Employed
- Unemployed
- Student
- Retired

5. **Duration of Using ABSA Mobile Banking:**
    - Less than 1 year
    - 1-3 years
    - 3-5 years
    - More than 5 years
6. **Frequency of Using ABSA Mobile Banking Platform:**
    - Daily
    - Weekly
    - Monthly
    - Rarely

Section B: To Analyse the Impact of Cybersecurity Breaches on User Trust in ABSA's Mobile Banking Services in Lusaka

7. **Have you ever experienced a cybersecurity breach while using ABSA's mobile banking platform?**
    - ☐ Yes
    - ☐ No

If no, please proceed to question 10.

8. **If yes, how did you become aware of the cybersecurity breach?** (You can select more than one option)
    - Received a notification from ABSA
    - Noticed unauthorized transactions
    - A friend or family member alerted me
    - Through news or social media
9. **Following the cybersecurity breach, how did your trust in ABSA's mobile banking services change?**
    - ☐ Greatly decreased
    - ☐ Somewhat decreased
    - ☐ Remained the same
    - ☐ Somewhat increased (e.g., due to rapid response by ABSA)
    - ☐ Greatly increased
10. **To what extent do you agree with the following statement: "ABSA takes adequate measures to protect its mobile banking users from cybersecurity threats"?**

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Neutral
- ☐ Agree
- ☐ Strongly Agree

11. **How often does cybersecurity concern influence your decision to use ABSA's mobile banking services?**

- ☐ Always
- ☐ Often
- ☐ Sometimes
- ☐ Rarely
- ☐ Never

12. **In case of a reported cybersecurity breach, which of the following actions by ABSA would most likely restore your trust?** (You can select more than one option)

- ☐ Immediate communication and acknowledgment of the breach
- ☐ Swift resolution of the breach and assurance that it won't recur
- ☐ Compensation for any potential financial loss
- ☐ Offering additional security features or upgrades
- ☐ None of the above

13. **Based on your experiences and knowledge, rate your level of trust in ABSA's mobile banking security protocols.**

- ☐ Very Low
- ☐ Low
- ☐ Moderate
- ☐ High
- ☐ Very High

SECTION C: 2. To Determine the Relationship between Frequency of Cybersecurity Incidents and User Engagement with ABSA's Mobile Money Platforms in Lusaka

14. **Considering any known cybersecurity incidents, how often do you engage with ABSA's mobile money platform?**

- ☐ Very Frequently
- ☐ Frequently
- ☐ Occasionally
- ☐ Rarely
- ☐ Never

15. **The more I hear about cybersecurity incidents, the more cautious I become in using ABSA's mobile money platform.**

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Neutral
- ☐ Agree
- ☐ Strongly Agree

16. **I would use ABSA's mobile money platform more often if I was assured of its cybersecurity measures.**

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Neutral
- ☐ Agree
- ☐ Strongly Agree

17. **The frequency of cybersecurity incidents influences my choice of mobile money platform.**

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Neutral
- ☐ Agree
- ☐ Strongly Agree

18. **I am likely to switch to a different mobile money platform if ABSA experiences frequent cybersecurity breaches.**

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Neutral
- ☐ Agree
- ☐ Strongly Agree

19. **I believe ABSA's mobile money platform is more secure than other competing platforms despite the incidents.**

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Neutral
- ☐ Agree
- ☐ Strongly Agree

20. **Frequency of using ABSA's mobile money platform would increase if there were fewer reports of cybersecurity incidents.**

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Neutral
- ☐ Agree
- ☐ Strongly Agree

SECTION D: 3. To Assess the Influence of Cybersecurity Breaches on the Financial Performance of ABSA's Mobile Banking Operations in Lusaka.

21. **I believe cybersecurity breaches have a significant impact on ABSA's operating costs.**

- ☐ Strongly Disagree

- ☐ Disagree
- ☐ Neutral
- ☐ Agree
- ☐ Strongly Agree

22. **In your opinion, do cybersecurity breaches lead to significant financial losses for ABSA?**

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Neutral
- ☐ Agree
- ☐ Strongly Agree

23. **I perceive that cybersecurity breaches have led to a decrease in ABSA's customer base.**

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Neutral
- ☐ Agree
- ☐ Strongly Agree

24. **How likely are cybersecurity breaches to affect ABSA’s stock/share price?**

- ☐ Very Unlikely

- ☐ Unlikely
- ☐ Neutral
- ☐ Likely
- ☐ Very Likely

25. **I would consider cybersecurity breaches as a primary factor when investing in ABSA shares.**

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Neutral
- ☐ Agree
- ☐ Strongly Agree

26. **Do you believe that cybersecurity breaches have a long-term impact on ABSA's profitability?**

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Neutral
- ☐ Agree
- ☐ Strongly Agree

27. **In your view, does ABSA invest adequately in cybersecurity measures to protect its financial health?**

- ☐ Strongly Disagree

- ☐ Disagree
- ☐ Neutral
- ☐ Agree
- ☐ Strongly Agree

Thank you for your valuable input on the influence of cybersecurity breaches on the financial performance of ABSA's mobile banking operations. Your responses are essential for the analysis of this study.

REFERENCES

Ajibade, P. (2018). Mobile Banking in Emerging Markets: A Global Perspective. Cambridge University Press.

Alalwan, A., Dwivedi, Y. K., Rana, N. P., & Algharabat, R. (2018). Examining factors influencing Jordanian customers' intentions and adoption of internet banking: Extending UTAUT2 with risk. Journal of Financial Service Marketing, 15(1), 22-37.

Al-Jenaibi, F. (2017). The role of cybersecurity in mobile banking. Journal of Advanced Research in Banking and Finance Technology, 2(1), 13-23.

Bain & Company. (2017). Customer Loyalty in Retail Banking. Bain & Company, Inc.

Bain & Company. (2017). Customer Loyalty in Retail Banking. Bain & Company, Inc.

Brigham, E.F., & Ehrhardt, M.C. (2013). Financial Management: Theory & Practice. Cengage Learning.

Bryman, A. (2016). Social research methods (5th ed.). Oxford University Press.

Chanda, N. (2021). Trust Dynamics in Zambia's Digital Financial Landscape. Zambian Financial Quarterly.

Chanda, N. (2021). Trust Dynamics in Zambia's Digital Financial Landscape. Zambian Financial Quarterly.

Chikoti, L. (2020). Cybersecurity Preparedness in Zambian Financial Institutions. Lusaka Financial Review, 27(3), 45-61.

Chikweche, T., & Fletcher, R. (2020). Understanding the mobile money adoption in the urban African context: Lessons from Lusaka. African Journal of Business Management, 14(3), 112-125.

Chimfwembe, L. H. (2020). Factors influencing the adoption of mobile banking in Zambia. International Journal of Bank Marketing.

Chimfwembe, L. H. (2021). Cybersecurity Concerns in Zambia's Mobile Banking Ecosystem. International Journal of Bank Marketing.

Chimfwembe, L. H. (2021). Cybersecurity Concerns in Zambia's Mobile Banking Ecosystem. International Journal of Bank Marketing.

Chimfwembe, L. H. (2021). Cybersecurity Concerns in Zambia's Mobile Banking Ecosystem. International Journal of Bank Marketing.

Creswell, J. W. (2014). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (4th ed.). SAGE Publications.

Creswell, J. W., & Plano Clark, V. L. (2017). Designing and Conducting Mixed Methods Research (3rd ed.). SAGE Publications.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. Management Science, 35(8), 982-1003.

Davis, F.D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319-340.

Demirgüç-Kunt, A., Klapper, L., Singer, D., & Van Oudheusden, P. (2015). The Global Findex Database 2014: measuring financial inclusion around the world. World Bank Policy Research Working Paper, (7255).

Demirgüç-Kunt, A., Klapper, L., Singer, D., & Van Oudheusden, P. (2018). The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution. World Bank Publications

Denzin, N. K., & Lincoln, Y. S. (2011). The SAGE Handbook of Qualitative Research (4th ed.). SAGE Publications.

Donovan, K. (2012). Mobile money for financial inclusion. Information and Communications for Development, 61-73.

FireEye. (2017). Advanced Persistent Threats: A Decade in Review. FireEye Inc.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. Journal of Applied Social Psychology, 30(2), 407-429.

Hardin, R. (2002). Trust and trustworthiness. Russell Sage Foundation.

ISO. (2016). ISO/IEC 27001 - Information Security Management. International Organization for Standardization.

Israel, M., & Hay, I. (2006). Research ethics for social scientists. SAGE Publications.

Juniper Research. (2019). Cybercrime & the Internet of Threats 2019. Juniper Research Limited.

Juniper Research. (2019). Cybercrime & the Internet of Threats 2019. Juniper Research Limited.

Juniper Research. (2019). Cybercrime & the Internet of Threats 2019. Juniper Research Limited.

Kabwe, F. (2021). User Interactions with Mobile Banking in Lusaka: A Behavioral Perspective. Zambian Journal of Technology and Culture, 15(2), 88-102.

Kabwe, P. (2018). Mobile banking in Zambia: Risks, perception, and mitigation. African Journal of Information Systems, 10(2).

Kaspersky. (2018). Mobile malware evolution 2018. Kaspersky Lab.

Kaspersky. (2018). Mobile malware evolution 2018. Kaspersky Lab.

Kaspersky. (2018). Mobile malware evolution 2018. Kaspersky Lab.

Kim, G., Shin, B., & Lee, H. G. (2018). Understanding dynamics between initial trust and usage intentions of mobile banking. Information Systems Journal, 28(3), 551-573.

Kim, G., Shin, B., & Lee, H. G. (2018). Understanding dynamics between initial trust and usage intentions of mobile banking. Information Systems Journal, 28(3), 551-573.

Mbiti, I., & Weil, D. N. (2016). Mobile banking: The impact of M-Pesa in Kenya. NBER Macroeconomics Annual, 30(1), 493-529.

Mcknight, D.H., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: a trust building model. The Journal of Strategic Information Systems, 11(3-4), 297-323.

Mertens, D. M., & Ginsberg, P. E. (2009). The Handbook of Social Research Ethics. SAGE Publications.

Moore, T., Dynes, S., & Johnson, A. (2016). The immediate costs of a major cybersecurity breach: A case study of Target Corp's 2013 data breach. Journal of Corporate Finance & Risk Management, 10(3), 56-69.

Mowery, D., Hull, G., & Ahmadi, M. (2019). Cybersecurity in the Digital Age: Tools, Strategies, and Best Practices. Palgrave Macmillan.

Mumba, K. (2021). The role of mobile money in financial inclusion in Zambia. Zambia Journal of Economics, 25(2), 45-60.

Mutale, F. (2020). The Hidden Costs of Cybercrime in Zambia's Financial Sector. Zambian Financial Review.

Mwale, S., & Sankalimodzi, J. (2019). Mobile Banking in Zambia: An Insight into Security Framework Adoption. African Journal of Information Systems, 11(1), 1-23.

Neuman, W. L., & Robson, K. (2014). Basics of social research: Qualitative and quantitative approaches (3rd Canadian ed.). Pearson Canada.

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology.

Nkwe, N. (2017). Cybersecurity Challenges in Developing Nations. African Journal of Computing & ICT, 10(5), 15-27.

O'Brien, H.L., & Toms, E.G. (2008). What is user engagement? A conceptual framework for defining user engagement with technology. Journal of the American Society for Information Science and Technology, 59(6), 938-955.

Oduro, I., Ahenkora, K., & Peprah, J. A. (2020). Understanding consumers' behavioural intention to adopt and use mobile banking in Ghana. Journal of African Business, 21(1), 105-128.

Oduro, I., Ahenkora, K., & Peprah, J. A. (2020). Understanding consumers' behavioural intention to adopt and use mobile banking in Ghana. Journal of African Business, 21(1), 105-128.

Oyediran, W. O., Olajide, D., & Sodiya, A. S. (2018). Analysis of mobile banking malware on android devices. International Journal of Cyber-Security and Digital Forensics, 7(4), 315-324.

PCI DSS. (2020). Payment Card Industry (PCI) Data Security Standard. PCI Security Standards Council.

Pfleeger, C.P., & Pfleeger, S.L. (2015). Security in Computing. Prentice Hall.

Phiri, D., & Nyirenda, J. (2022). Socio-economic implications of mobile money platforms in Zambia. African Economic Review, 30(1), 28-44.

Reichheld, F.F. (2001). Loyalty Rules: How Today's Leaders Build Lasting Relationships. Harvard Business Press.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2(2), 121-135.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2(2), 121-135.

Saunders, M., Lewis, P., & Thornhill, A. (2016). Research Methods for Business Students (7th ed.). Pearson.

Shaikh, A. A., & Karjaluoto, H. (2015). Mobile banking adoption: A literature review. Telematics and Informatics, 32(1), 129-142.

Silverman, D. (2016). Qualitative Research (4th ed.). SAGE Publications.

Smith, A., Dinev, T., & Xu, H. (2011). Information privacy and trust in mobile banking. Journal of Cybersecurity and Banking, 5(2), 123-137.

Sohail, M. S., & Al-Jabri, I. M. (2014). Mobile banking adoption: Application of diffusion of innovation theory. Journal of Electronic Commerce Research, 15(4), 280-301.

Symantec. (2020). Internet Security Threat Report. Symantec Corporation.

Mumba, S., & Nkonde, C. (2018). User Trust and Cybersecurity in Mobile Banking: The Role of Communication. Journal of Financial Cybersecurity, 4(2), 67-82.

Chileshe, M., & Chanda, F. (2019). The Impact of Security Breach Notifications on Customer Trust: A Zambian Perspective. Zambian Journal of Banking Technology, 6(1), 45-60.

Kabaso, L., & Phiri, J. (2020). Post-Breach Transformations in Bank Cybersecurity Strategies. African Journal of Banking and Finance, 12(3), 115-130.

Lungu, E., & Sikazwe, G. (2021). Regulatory Influences on Cybersecurity in the Zambian Banking Sector. Journal of Financial Regulation in Zambia, 8(4), 200-215.

Musonda, I., & Tembo, N. (2022). Corporate Demands for Bank Cybersecurity: A Zambian Market Analysis. Journal of Corporate Banking and Security, 10(2), 134-147.Watson, J. (2019). Cyber Breaches and Customer Loyalty. Financial Times.

Watson, J. (2019). Cyber Breaches and Customer Loyalty. Financial Times.

Yin, R. K. (2013). Case study research: Design and methods. SAGE Publications.

Zhou, T. (2012). The impact of privacy concern on user adoption of mobile banking. Journal of Modern Banking Systems, 6(4), 29-41.

Zhou, T. (2019). Examining mobile banking user loyalty from the perspectives of trust and flow experience. Computers in Human Behavior, 95, 208-220.

Zhou, T. (2019). Examining mobile banking user loyalty from the perspectives of trust and flow experience. Computers in Human Behavior, 95, 208-220.

Zhou, T., Lu, Y., & Wang, B. (2010). Integrating TTF and UTAUT to explain mobile banking user adoption. Computers in Human Behavior, 26(4), 760-767.

ZICTA. (2019). Annual Cybersecurity Threat Intelligence Report. Zambian Information and Communication Technology Authority.

ZICTA. (2019). Annual Cybersecurity Threat Intelligence Report. Zambian Information and Communication Technology Authority.

ZICTA. (2019). Annual Cybersecurity Threat Intelligence Report. Zambian Information and Communication Technology Authority.