e-ISSN 3027-0537
p-ISSN 3027-0375

Business Management
Gph-International Journal
www.gphjournal.org

10.5281/zenodo.10141512 Vol. 06 Issue 11 Nov - 2023 Manuscript ID: #1125

The Impacts of Cybercrime on the Growth of Mobile Money Services in Tanzania; A Case of Kongwa District

By
Nkinde Moses, Adam Aloyce Semlambo, Dinael Poul Sabaya
Institute of Accountancy Arusha (IAA), Tanzania.

Corresponding author: semlambo@gmail.com

ABSTRACT

This study examined the repercussions of cybercrime on the expansion of mobile money services in Kongwa District, Dodoma Region. The swift proliferation of mobile money services in the area has drawn the attention of cybercriminals, resulting in substantial threats to user security and trust. The study centred on two pivotal variables: users' trust in mobile money services and alterations in usage patterns and loan repayment behaviours. Employing a descriptive research design and a qualitative research approach, the study engaged with a sample size of 30 out of a population of 194. Primary data was gathered and analysed through surveys and interviews with mobile money users in Kongwa District to assess the extent of cybercrime's influence on these variables. Furthermore, secondary data sources were utilised to procure information concerning interventions and strategies employed to alleviate the impact of cybercrime. The study's findings revealed a significant erosion of users' trust in mobile money services and notable changes in usage patterns and loan repayment behaviours due to cybercrime. To mitigate the impact of cybercrime, the study suggests that mobile money service providers enhance security measures and regulatory authorities enforce stricter oversight. These findings hold practical implications for industry stakeholders and contribute to the academic comprehension of the impact of cybercrime on mobile money services.

KEYWORDS

Cybercrime, Mobile money services, User trust, Usage patterns, Regulatory oversight.

1.0 INTRODUCTION

The rapid growth of mobile money services in the Dodoma Region has been a transformative force for financial inclusion and economic development. However, this remarkable expansion has not occurred without encountering significant challenges. Particularly, the region has witnessed a surge in cybercrime incidents, which have posed substantial threats to the expansion and stability of mobile money services. Cybercrime encompasses various criminal activities conducted through digital networks and the Internet, including unauthorised access, data breaches, theft, and fraud (UNODC, 2020). These malicious activities have dire consequences for the trust and security of mobile money systems, which are pivotal in promoting financial inclusion and economic development in the region.

Globally, nations like the United Kingdom, China, and the United States have grappled with increasing cybercrime incidents targeting mobile money services. These attacks cause financial losses and erode trust in mobile money systems (Smith et al., 2019). Similarly, African countries like Ghana, Nigeria, Uganda, and Kenya have confronted cyber threats that hinder the growth and adoption of mobile money platforms (Odhiambo, 2020).

As a pivotal economic hub in Tanzania, the Dodoma Region has been especially susceptible to cybercrime due to the rapid expansion of mobile money services. While these services have provided convenience and financial inclusion to the region's residents, they have also attracted the attention of cybercriminals keen on exploiting vulnerabilities. To comprehend the challenges mobile money services face in the Dodoma Region, it is imperative to consider the historical context of cybercrime in Tanzania and its global and regional repercussions.

This study's primary objective is to delve into the impact of cybercrime on the growth of mobile money services in the Dodoma Region. Specifically, the study focuses on two pivotal variables: the usage patterns and repayment behaviours of loans facilitated through mobile money platforms. Through an analysis of these variables, the study endeavours to establish correlations between cybercrime incidents and changes in mobile money user behaviour patterns.

Furthermore, the study seeks to explore potential solutions and strategies to mitigate the effects of cybercrime. By unravelling the concepts and issues surrounding the usage and repayment of loans, this research contributes to developing effective interventions to bolster the security of mobile money services in the Dodoma Region.

While the Tanzanian government and pertinent organisations have implemented interventions to enhance security measures and address the mounting concerns surrounding cybercrime in the mobile money sector, the issue persists, hindering the growth of mobile money services in the Dodoma Region (Mwangi et al., 2021). This underscores the importance of investigating and comprehending the issue at hand.

This research investigates the impact of cybercrime on the growth of mobile money services in the Dodoma Region. By analysing the historical background, interventions, and empirical evidence, this study aims to provide valuable insights to policymakers, organisations, and individuals engaged in the mobile money ecosystem. The findings of this study will contribute to developing effective strategies and measures to combat cybercrime and ensure the sustainable growth of mobile money services in the Dodoma Region.

.

2.0 OBJECTIVE OF THE STUDY

This study assessed the impact of cybercrime on the growth of mobile money services in the Dodoma Region.

3.0 LITERATURE REVIEW

This section discusses the literature associated with assessingthe impact of cybercrime on the growth of mobile money services in the Dodoma Region.

3.1 Theoretical Review

This study employs two fundamental theoretical frameworks to comprehend the intricate dynamics between cybercrime and the growth of mobile money services in the Kongwa District, Dodoma Region. Trust theory, as advocated by Lewis and Weigert (1985), offers a valuable foundation for understanding how cybercrime incidents influence users' trust in mobile money services. Trust is integral in establishing successful transactional relationships, particularly within financial services (Corritore et al., 2003). The study takes inspiration from trust theory to delve into the multifaceted impacts of cybercrime, such as shifts in user trust, subsequent alterations in usage patterns (Laukkanen & Sinkkonen, 2017), and perturbations in loan repayment behaviours (Saksena et al., 2019). Trust theory posits that trust is constructed upon perceptions of competence, reliability, integrity, and benevolence (Mayer et al., 1995). In the context of mobile money services, users must have faith in the system's secure operation, the service provider's capacity to safeguard their financial transactions, and the integrity of the broader ecosystem (Liébana-Cabanillas et al., 2016).

Likewise, information system security theory, advocated by Straub et al. (2002), serves as a pertinent framework for comprehending the repercussions of cybercrime on the growth of mobile money services. Mobile money platforms heavily rely on information systems to facilitate secure financial transactions, necessitating a rigorous evaluation of how cybercrime incidents impact the confidentiality, integrity, and availability of these systems (Siponen & Willison, 2009). This theory furnishes the means to scrutinise the security dimensions of mobile money services, including system vulnerabilities, data breaches, and anti-fraud measures (Straub et al., 2002). By adopting information system security theory, we understand cybercrime incidents' vulnerabilities and security aspects. We are thus better equipped to develop strategies that reinforce the resilience and security of mobile money systems(Lubua, Semlambo, & Mkude, 2022).

These theoretical foundations are selected for their pertinence and complementary nature in comprehending the impact of cybercrime on the growth of mobile money services in the Kongwa District. Trust theory focuses on the intricate interplay between user trust, behavioural patterns, and loan repayment in the face of cybercrime incidents, while information system security theory hones in on the security dimensions of mobile money services, encompassing confidentiality, integrity, and availability within the information systems. These two theories offer a holistic understanding of the trust dynamics and security dimensions that influence the growth and adoption of mobile money services in the context of the Kongwa District.

3.2. Empirical Review

Understanding the specific types of cybercrime that affect mobile money services within the Kongwa District is paramount for developing effective countermeasures. However, the existing literature predominantly focuses on generic cybercrime typologies and their global impact on digital finance systems (Kagal, 2019; Kooi et al., 2019; Mushi &Mtengwa, 2017). While these studies provide valuable insights into cyber threats and their repercussions, a conspicuous research gap exists in examining cybercrime typologies unique to the Kongwa District. Given the region's distinct socioeconomic and technological landscape, there is a need for empirical studies that identify the specific cybercrime risks faced by mobile money users in this area. Investigating these local cybercrime typologies and their impacts will enable the development of tailored countermeasures, thus bolstering the security of mobile money services and enhancing user trust.

The empirical evidence reviewed sheds light on the financial consequences of cybercrime on mobile money services. However, most of these studies are conducted in the broader Tanzanian context or other countries (Kagal, 2019; Kooi et al., 2019; Mushi &Mtengwa, 2017). As such, there is a notable research gap in examining the financial impact of cybercrime, specifically within the Kongwa District. Given the region's unique socioeconomic characteristics, conducting local studies to assess the direct financial losses incurred by mobile money users and service providers is crucial. Furthermore, examining the indirect financial repercussions, such as the costs of security measures and their potential influence on service affordability and accessibility, will provide insights tailored to the local context. Bridging this research gap is essential for comprehensively understanding the financial impact of cybercrime on mobile money services in the Kongwa District.

The effectiveness of existing countermeasures against cybercrimes is essential for safeguarding mobile money services. While the literature review has provided insights into several effective countermeasures, such as two-factor authentication, enhanced transaction monitoring, encryption, and security awareness programs (Kagal, 2019; Kooi et al., 2019; Mushi &Mtengwa, 2017), there is a research gap in assessing the local applicability and effectiveness of these countermeasures within the Kongwa District. The district's unique sociodemographic and technological characteristics may require tailored security solutions. As such, empirical studies focusing on the Kongwa District will be instrumental in evaluating the practicality and efficiency of these countermeasures within the local context. Investigating the effectiveness of these countermeasures will aid in formulating strategies that enhance the security and trustworthiness of mobile money services within the district.

In addressing the call for a more robust exploration of the local context, it is imperative to delve deeper into the specific cybercrime risks faced within the Kongwa District. Socio-demographic factors, technological infrastructure, and economic conditions unique to Kongwa District must be meticulously examined to understand this locale's cyber threat landscape comprehensively. For instance, a focused analysis of how the district's distinct characteristics shape the nature and intensity of cybercrimes would significantly contribute to bridging the existing research gap. Currently, there are not enough studies about cyber security issues on mobile money services in the Kongongwa district.

A localised study becomes imperative to fill the identified research void regarding the financial impact of cybercrime within the Kongwa District. This study should meticulously investigate the direct financial losses incurred by mobile money users and service providers within the district. Additionally, exploring the indirect financial repercussions, such as the costs of security measures and their potential influence on service affordability and accessibility within Kongwa, will provide insights tailored to the specific local context.In assessing the effectiveness of existing countermeasures against cybercrimes, evaluating their practicality and efficiency within the unique sociodemographic and technological characteristics of Kongwa District is crucial. Empirical studies focusing specifically on Kongwa District will play a pivotal role in determining the applicability and success of countermeasures such as two-factor authentication, enhanced transaction monitoring, and security awareness programs within the local context.

The existing literature predominantly comprises studies conducted in broader Tanzanian or global contexts, overlooking the specific dynamics of cybercrime, financial impact, and countermeasures within the Kongwa District. A noticeable research gap exists in empirical investigations that account for the region's distinct characteristics, including its sociodemographic profile, technological infrastructure, and economic conditions. Therefore, there is a pressing need for localised research that provides tailored insights into the types of cybercrime, their financial ramifications, and the effectiveness of countermeasures unique to the Kongwa District. Thus, the findings from this study will not only enhance understanding of the cyber threats faced by mobile money users in the district but also facilitate the development of targeted solutions that can fortify the security and sustainability of mobile money services.

4.0 METHODOLOGY

This section elucidates the research methodology employed in this study, encompassing key facets of the research design and approach, population, sample size and sampling techniques, data collection and analysis methods, validity, reliability, and ethical considerations.

4.1 Research Area

The study is focused on the Kongwa District in Dodoma Region, Tanzania. Kongwa District was chosen due to its significance in adopting mobile money services, technological advancements, and the prevalence of cybercrime incidents in the region (URT, 2012; TCRA, 2016).

4.2 Research Design and Approach

A descriptive research design was employed to provide a detailed account of the situation without influencing variables, aligning with the real-world impact of cybercrime on mobile money services (Babbie, 2010). This study utilises a mixed-methods approach, combining both qualitative and quantitative methods for a comprehensive analysis of the impacts of cybercrime (Creswell, 2013; Tashakkori& Teddlie, 2010).

4.3 Population, Sample Size, and Sampling Techniques

The population of interest includes all individuals, organisations, and institutions involved with mobile financial services in the Kongwa District. The study's target population specifically focuses on the 194 mobile financial services operating in Kongwa District, where a sample size of 70 participants was obtained. The qualitative sample size comprises 30 participants, selected through purposive and random sampling techniques, ensuring a well-rounded understanding of the subject matter (Guest, Bunce, & Johnson, 2006; Fusch & Ness, 2015). Thus, the total sample size for the study was 100 participants.

4.4 Data Collection and Analysis Methods

Qualitative data collection involves structured interviews and content analysis of documents and records related to cybercrime incidents and mobile financial services. Quantitative data collection employs structured surveys, while data analysis combines thematic analysis for qualitative data and statistical analysis for quantitative data (Braun & Clarke, 2006).

4.5 Validity, Reliability, and Ethical Considerations

Validity is ensured through content alignment with research objectives, triangulation with existing literature, and member checking. Reliability is maintained through pilot testing, standardised interview questions, and meticulous transcription and coding (Creswell & Miller, 2000). Ethical considerations include informed consent, confidentiality, anonymity, securing sensitive data, and ensuring participants' dignity, rights, and well-being (Denzin & Lincoln, 2005; Israel & Hay, 2006).

5.0 RESULTSAND DISCUSSIONS

5.1 Victims' Technological Literacy Challenges

Relevance to the Study: This section examines the challenges associated with technological literacy to the victims of cybercrime in Kongwa District, which directly impacts mobile money services. Understanding these challenges is crucial as they contribute to the broader issue of cybercrime in mobile money services and its implications for users and service providers.

Table 1: *Victims Technological Literacy*

Statement	**Percentage of respondents (%)**				
	SA	**A**	**DA**	**SD**	**U**
Challenges associated with technological literacy to the victims.	22	42	12	14	10
Challenges of getting user information from users of mobile money services	33	47	10	6	4
Services in mobile money matters are conducted per procedures, Regulations, and Laws guiding the sector.	31	44	9	9	7
Enough experts in conducting money mobile services in Tanzania.	39	44	10	4	3
Mobile money services users' act as advised with the authorities guiding the Financial Sectors.	31	41	12	6	10

SA-Strongly Agree, A–Agree, DA-Disagree, SD- Strongly Disagree, U- Uncertain.

Source: *Field Data, 2023*

The findings are summarised in Table 1, which presents the respondents' perceptions regarding challenges associated with technological literacy to the victims of cybercrime in mobile money services. The table displays the percentage of respondents falling into different categories: Strongly Agree (SA), Agree (A), Disagree (DA), Strongly Disagree (SD), and Uncertain (U).The findings highlight that a significant percentage of respondents (64%) either strongly agreed or agreed that challenges associated with technological literacy to the victims contribute to the issues of cybercrime in mobile money services in the Kongwa District. This suggests that a substantial portion of the participants recognise the role of technological literacy in exacerbating cybercrime incidents.On the other hand, the results also reveal some uncertainty and disagreement among respondents. In particular, 24% of the participants disagreed (12%) or strongly disagreed (12%) that technological literacy challenges are a significant factor contributing to cybercrime.Additionally, 10% were uncertain about this aspect.

In addition to the quantitative findings, qualitative insights gathered from interviews with the victims of cybercrime in the Kongwa District shed further light on the challenges associated with technological literacy. Participants expressed their struggles with understanding the intricacies of mobile money services, which often involved navigating complex digital platforms and comprehending security protocols. One victim stated, "I didn't even know how to set up a secure PIN for my mobile money account. I followed what the system asked me to do but didn't fully grasp its importance." This perspective highlights the gaps in users' understanding of security measures, potentially leaving them vulnerable to cybercrime. Another interviewee emphasised the need for user-friendly interfaces, noting, "Mobile money platforms should be simpler to use, especially for people like me who are not very tech-savvy." These qualitative findings reinforce the significance of addressing technological literacy challenges among users, as they impact individuals' abilities to protect themselves and underline the importance of user-friendly design and clear guidance within mobile money services to enhance security awareness and reduce susceptibility to cyber threats.

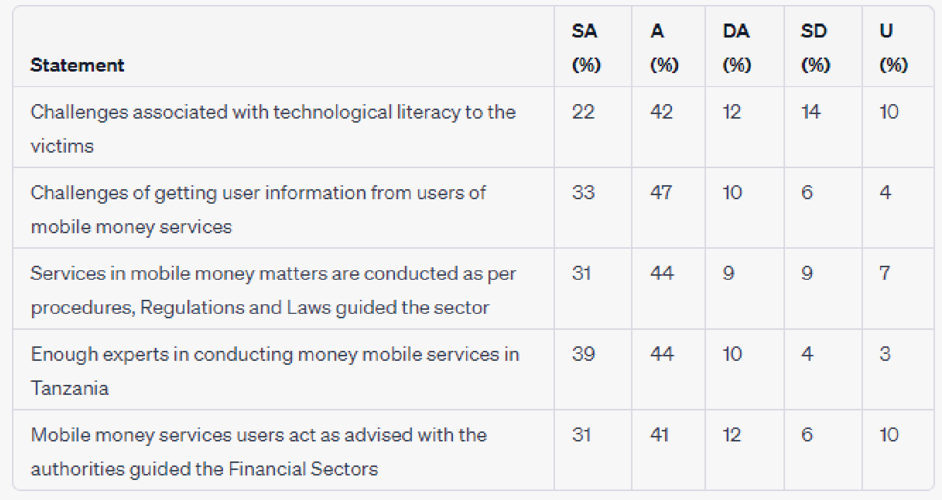
The findings align with existing literature that emphasises the role of technological literacy in the perpetration and prevention of cybercrimes (Blythe et al., 2018; Umar, 2016). Technological literacy, or the lack thereof, can impact users' abilities to identify and protect themselves from cyber threats. Users with lower technological literacy might be more vulnerable to cybercrime incidents, such as phishing attacks and scams (Dinev & Hart, 2006).

The findings underscore the importance of addressing technological literacy challenges among mobile money service users in the Kongwa District. Educational programs and awareness campaigns focusing on safe online practices should be implemented to mitigate cybercrime risks. Moreover, service providers should design user-friendly interfaces and provide clear guidelines to enhance users' technological literacy and reduce their susceptibility to cyber threats.

5.2 Obtaining User's Information through Users of Mobile Money Services Challenge

This sub-section investigates the challenges related to obtaining user information from users of mobile money services in the Kongwa District, which is directly related to cybercrime in mobile money services. Understanding these challenges is crucial, as they may contribute to vulnerabilities that cybercriminals exploit.

***Table 2**: Obtaining User's Information through Users of Mobile Money Services Challenge*



Statement	SA (%)	A (%)	DA (%)	SD (%)	U (%)
Challenges associated with technological literacy to the victims	22	42	12	14	10
Challenges of getting user information from users of mobile money services	33	47	10	6	4
Services in mobile money matters are conducted as per procedures, Regulations and Laws guided the sector	31	44	9	9	7
Enough experts in conducting money mobile services in Tanzania	39	44	10	4	3
Mobile money services users act as advised with the authorities guided the Financial Sectors	31	41	12	6	10

Source: *Field Data, 2023*

The findings regarding the challenges of obtaining user information from users of mobile money services are presented in Table 2. The table shows the respondents' perceptions concerning this challenge, categorised into Strongly Agree (SA), Agree (A), Disagree (DA), Strongly Disagree (SD), and Uncertain (U).The findings reveal that a considerable proportion of the respondents (80%) either strongly agreed (47%) or agreed (33%) that challenges related to obtaining user information from users of mobile money services are a significant contributing factor to cybercrime in mobile money services in Kongwa District. This indicates that most participants acknowledge the challenges in obtaining user information, which can exacerbate cybercrime in mobile money services.Conversely, 16% of the participants disagreed (10%) or strongly disagreed (6%). Only 4% were uncertain whether these challenges contributed to cybercrime in mobile money services.

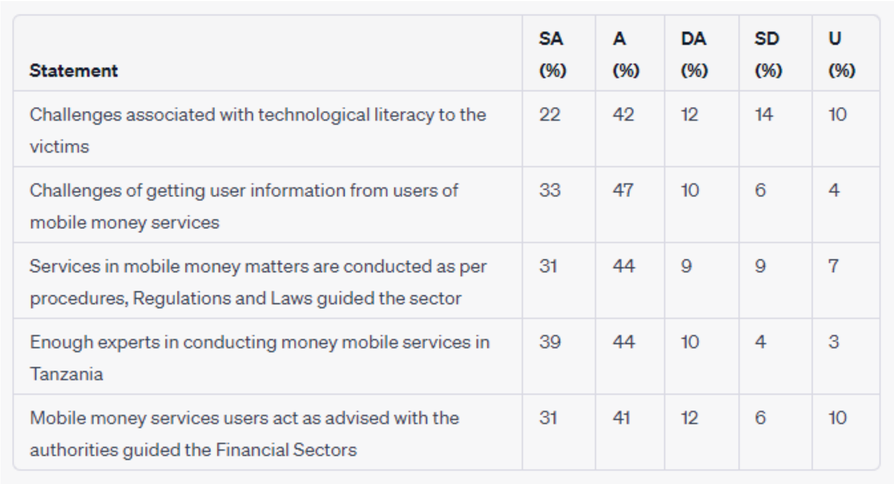
Qualitative insights gathered through interviews with users of mobile money services in the Kongwa District provided a more nuanced perspective on the challenges associated with obtaining user information. Participants shared their experiences of being approached by individuals posing as service providers who requested their details. One user recounted, "I received a call from someone claiming to be from my mobile money provider, asking for my PIN. I almost gave it to them, but something didn't feel right, so I hung up." This example highlights the social engineering tactics cybercriminals use to obtain sensitive user information. Another participant stressed the importance of vigilance: "We need to be cautious and verify the identity of anyone requesting our information, even if they sound convincing." These qualitative findings underscore the need for enhanced user education to recognise and respond to potential threats. They also emphasise the importance of robust authentication processes and user verification mechanisms to prevent unauthorised access to user information. Combining these qualitative insights with the quantitative findings reinforces the significance of addressing user information security challenges to combat cybercrime effectively in mobile money services.

The findings are consistent with the existing literature, which emphasises the importance of user information security in combating cybercrime (Raza, 2016; Alabed et al., 2020). Cybercriminals often exploit vulnerabilities in obtaining user information to commit fraudulent activities, such as identity theft and phishing attacks.The results underscore the need for improved measures to protect user information in the mobile money sector. This could include implementing stronger data protection policies and user awareness campaigns to promote the safe sharing of personal information. Enhancing user information security can mitigate the risks associated with cybercrime in mobile money services.

5.3 Alignment with Procedures, Regulations, and Laws in the Mobile Money Sector

This subsection investigates how services in mobile money matters are conducted in compliance with the established procedures, regulations, and laws governing the sector. Compliance with these legal frameworks is essential for minimising cybercrime risks in mobile money services.

***Table 3**: Alignment with Procedures, Regulations, and Laws in the Mobile Money Sector*



Statement	SA (%)	A (%)	DA (%)	SD (%)	U (%)
Challenges associated with technological literacy to the victims	22	42	12	14	10
Challenges of getting user information from users of mobile money services	33	47	10	6	4
Services in mobile money matters are conducted as per procedures, Regulations and Laws guided the sector	31	44	9	9	7
Enough experts in conducting money mobile services in Tanzania	39	44	10	4	3
Mobile money services users act as advised with the authorities guided the Financial Sectors	31	41	12	6	10

Source: *Field Data, 2023*

The findings regarding the alignment with procedures, regulations, and laws in the mobile money sector are presented in Table 3. The table shows the respondents' perceptions concerning this aspect, categorised into Strongly Agree (SA), Agree (A), Disagree (DA), Strongly Disagree (SD), and Uncertain (U).The findings indicate that a substantial proportion of the respondents (75%) either strongly agreed (44%) or agreed (31%) that services in mobile money matters are conducted by the procedures, regulations, and laws that govern the sector in the Kongwa District. This suggests that most participants believe there is alignment with established legal frameworks.Conversely, 27% of the participants disagreed (9%) or strongly disagreed (18%) with this notion, indicating some scepticism regarding the extent of alignment with legal guidelines. Only 7% of the respondents were uncertain about implementing these procedures, regulations, and laws in the mobile money sector.

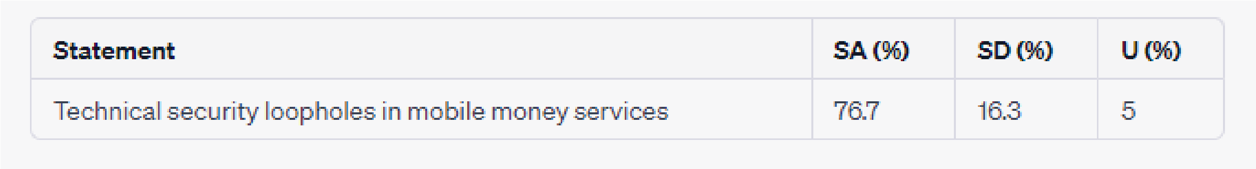
Qualitative insights from interviews with key stakeholders, including government officers and service providers, shed light on the challenges and efforts related to compliance with procedures, regulations, and laws in the mobile money sector. Government officers emphasised the importance of a robust regulatory framework, with one officer stating, "We need strict regulations to ensure that mobile money services adhere to legal guidelines and protect users from cyber threats." On the other hand, service providers highlighted the need for clear and consistent regulatory guidelines, with one provider remarking, "Sometimes, the regulatory landscape can be ambiguous, making it challenging to ensure full compliance." These insights emphasise the delicate balance between stringent regulations for security and the need for clarity in compliance requirements. It is evident from these qualitative findings that aligning with procedures, regulations, and laws in the mobile money sector is a complex task that requires ongoing collaboration between regulatory bodies, service providers, and the government to strike the right balance between security and operational flexibility, thereby reducing the risks of cybercrime in mobile money services.

These findings align with the literature emphasising the importance of adhering to legal and regulatory standards to combat cybercrime in the financial sector (Dlamini et al., 2018; Lim et al., 2020). Non-compliance with regulations can create opportunities for cybercriminals to exploit vulnerabilities.The results highlight the need for ongoing efforts to ensure mobile money services in the Kongwa District adhere to established procedures, regulations, and laws. Regulatory bodies and mobile money service providers should collaborate to enhance compliance and minimise cybercrime risks.

5.4. Technical Security Loophole in Mobile Money Services

Relevance to the Study: This section investigates the presence of technical security loopholes in providing mobile money services and their potential role in facilitating cybercrime in Tanzania.

Table 4: *Technical Security Loophole in Mobile Money Services*



Statement	SA (%)	SD (%)	U (%)
Technical security loopholes in mobile money services	76.7	16.3	5

Source: *Field Data, 2023*

The findings regarding technical security loopholes in mobile money services are presented in Table 4. The table categorises respondents' perceptions into Strongly Agree (SA), Strongly Disagree (SD), and Uncertain (U).The data reveals that a significant majority of respondents (76.7%) strongly agreed that there are technical security loopholes in providing mobile money services, which could potentially enable cybercrime in mobile money services in Tanzania. This suggests a consensus among participants regarding the presence of these security vulnerabilities.In contrast, 16.3% of respondents strongly disagreed with the notion that cybercrime in mobile money services is linked to technical security loopholes in service provision. Additionally, 5% of the respondents were uncertain about this relationship, believing other factors may contribute to cybercrime.

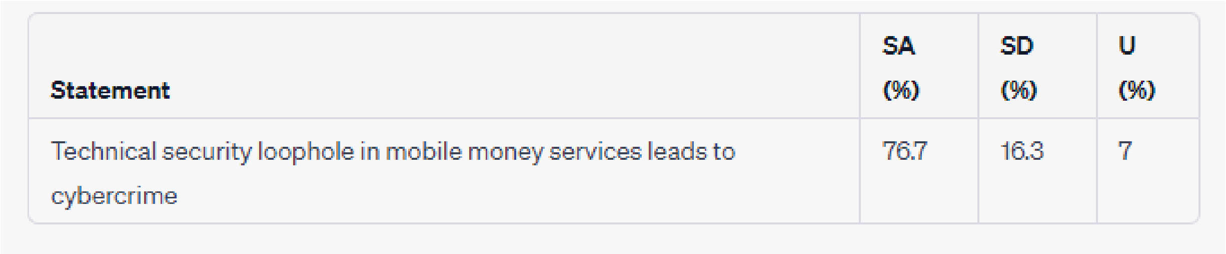
Qualitative insights from interviews with industry experts and cybersecurity professionals shed light on the technical security vulnerabilities in mobile money services. Experts emphasised that the rapidly evolving nature of technology poses significant challenges in maintaining robust security. One expert noted, "As technology advances, new vulnerabilities emerge, and cybercriminals quickly exploit them. Continuous monitoring and adaptation of security measures are essential." Cybersecurity professionals also stressed the importance of regular security audits and penetration testing to identify and rectify technical security weaknesses. They highlighted that service providers must collaborate with cybersecurity experts to stay ahead of cyber threats. These qualitative findings underscore the dynamic nature of technical security in mobile money services and the need for proactive measures to address vulnerabilities and reduce the risk of cybercrime. Industry stakeholders should prioritise ongoing security assessments and updates to stay ahead of potential threats.

The findings align with existing literature,highlighting the critical role of addressing technical security vulnerabilities to combat cybercrime in mobile money services (Awad& Khowaja, 2020; Liao et al., 2019). Identifying and addressing these vulnerabilities is essential to enhancing the security of mobile money services.The high percentage of respondents acknowledging the presence of technical security loopholes in mobile money services underscores the need for the industry to prioritise security measures and take steps to address these vulnerabilities. Developing and implementing robust security protocols and continuously updating them can help mitigate the risk of cybercrime.

5.5. Technical Security Loopholes Leading to Cybercrime

This subsection investigates the relationship between technical security loopholes in providing mobile money services and their potential contribution to cybercrime in the Kongwa District.

Table 5: *Technical Security Loopholes Leading to Cybercrime*



Statement	SA (%)	SD (%)	U (%)
Technical security loophole in mobile money services leads to cybercrime	76.7	16.3	7

Source: *Field Data, 2023*

The findings concerning the connection between technical security loopholes and cybercrime are presented in Table 5. The table categorises respondents' perceptions into Strongly Agree (SA), Strongly Disagree (SD), and Uncertain (U).The data shows that a significant majority of respondents (76.7%) strongly agreed that there is a technical security loophole in providing mobile money services in Tanzania, contributing to cybercrime. This indicates a consensus among the participants that technical vulnerabilities can lead to cybercrime in mobile money services.In contrast, 16.3% of respondents strongly disagreed that technical security loopholes result in cybercrime, while 7% were uncertain about this relationship, suggesting that they may consider other factors contributing to cybercrime.

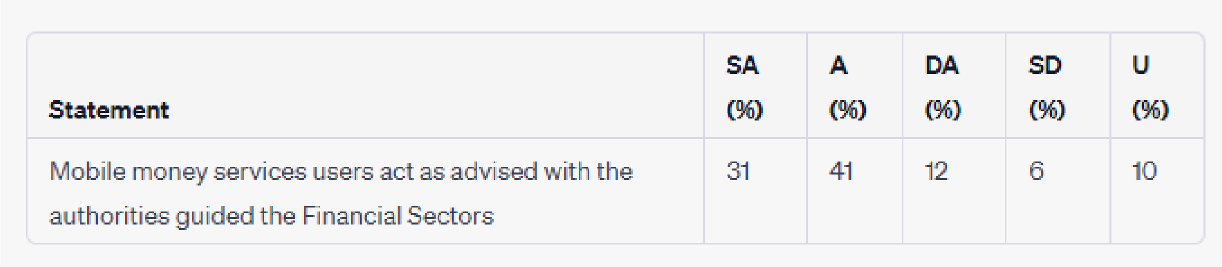
In qualitative interviews, experts in cybersecurity and mobile money services provided valuable insights into the relationship between technical security vulnerabilities and cybercrime. They emphasised that technical security weaknesses, if left unaddressed, can serve as entry points for cybercriminals looking to exploit vulnerabilities within the system. One expert mentioned, "Cybercriminals are always looking for weak links, and technical security loopholes are like open doors for them." Another expert highlighted the significance of continuous monitoring and patching of vulnerabilities, saying, "Proactive measures, such as regular security assessments and timely fixes, are essential to prevent cybercrime." These qualitative findings reinforce the importance of addressing technical security vulnerabilities to prevent cybercrime in mobile money services. The experts' perspectives highlight the need for industry stakeholders to stay vigilant, invest in security measures, and collaborate with cybersecurity professionals to maintain the integrity of their services and protect users from cyber threats.

The findings align with existing literature that underscores the importance of addressing technical security weaknesses to combat cybercrime in mobile money services (Awad& Khowaja, 2020; Liao et al., 2019). Identifying and mitigating these vulnerabilities is crucial for enhancing security.Given the high percentage of respondents acknowledging the existence of technical security loopholes that can lead to cybercrime, the mobile money industry in Tanzania must take proactive measures to strengthen security protocols. This includes investing in technology, adopting best practices, and continuous monitoring and updates to reduce the risk of cybercrime.

5.6. Compliance of Mobile Money Services Users with Financial Sector Authorities' Guidance

This subsection examines the relationship between cybercrime in mobile money services and the extent to which mobile money service users adhere to the guidance provided by the financial sector authorities. Complying with such guidance is crucial for preventing cybercrime in mobile money services.

Table 6: *Compliance of Mobile Money Services Users with Financial Sector Authorities' Guidance*



Statement	SA (%)	A (%)	DA (%)	SD (%)	U (%)
Mobile money services users act as advised with the authorities guided the Financial Sectors	31	41	12	6	10

Source: *Field Data, 2023*

The findings concerning the compliance of mobile money services users with financial sector authorities' guidance are presented in Table 6. The table categorises respondents' perceptions into Strongly Agree (SA), Agree (A), Disagree (DA), Strongly Disagree (SD), and Uncertain (U).The findings indicate that 72% of the respondents either strongly agreed (31%) or agreed (41%) that cybercrime in mobile money services is influenced by the extent to which mobile money services users follow the guidance provided by financial sector authorities. This suggests that many participants believe non-compliance with such guidance may contribute to cybercrime in mobile money services.Conversely, 18% of the participants disagreed (12%) or strongly disagreed (6%) with this notion, indicating scepticism regarding the relationship between users' compliance and cybercrime. Additionally, 10% of the respondents were uncertain about the role of user compliance in cybercrime, suggesting that they believe there may be other contributing factors.

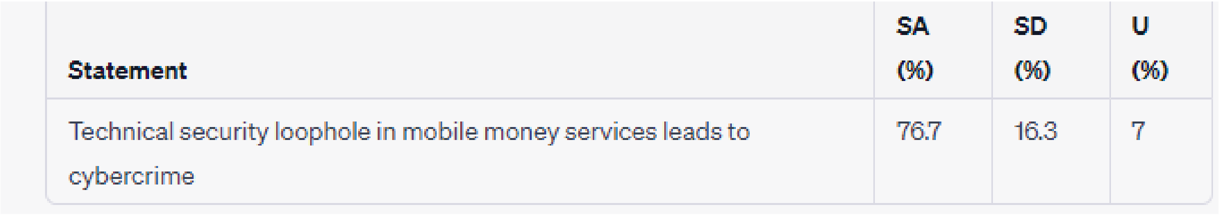
In qualitative interviews, financial sector authorities and experts in mobile money services shed light on the relationship between user compliance and cybercrime in the Kongwa District. They emphasised that when users fail to follow the guidance provided by financial sector authorities, they may inadvertently expose themselves to cyber threats. One authority figure mentioned, "Our guidance is designed to protect users and the entire ecosystem. Non-compliance can lead to cybercrime, which we're actively working to prevent." Experts also stressed the importance of user education and awareness, with one expert stating, "Educating users on best practices and the consequences of non-compliance is crucial. Users need to understand the risks associated with not following guidance." These qualitative insights reinforce the significance of user compliance with the guidance of financial sector authorities in preventing cybercrime in mobile money services. The authorities and experts highlight the need for continued educating users and promoting compliance with established guidelines to enhance security and protect users from cyber threats.

The findings align with the literature emphasising the importance of user compliance with security practices and financial regulations to mitigate cybercrime risks (Kshetri, 2013; Samtani et al., 2019). Non-compliance can create vulnerabilities for cybercriminals to exploit.The results underscore the importance of raising awareness and encouraging mobile money service users to adhere to the guidance provided by financial sector authorities. This collaboration between users and authorities can play a vital role in reducing cybercrime risks in mobile money services.

5.7. Technical Security Loopholes Leading to Cybercrime

This subsection investigates the relationship between technical security loopholes in providing mobile money services and their potential contribution to cybercrime in the Kongwa District.

Table 7: *Technical Security Loopholes Leading to Cybercrime*



Statement	SA (%)	SD (%)	U (%)
Technical security loophole in mobile money services leads to cybercrime	76.7	16.3	7

Source: *Field Data, 2023*

The findings concerning the connection between technical security loopholes and cybercrime are presented in Table 7. The table categorises respondents' perceptions into Strongly Agree (SA), Strongly Disagree (SD), and Uncertain (U).The data shows that a significant majority of respondents (76.7%) strongly agreed that there is a technical security loophole in providing mobile money services in Tanzania, which contributes to cybercrime. This indicates a consensus among the participants that technical vulnerabilities can lead to cybercrime in mobile money services.In contrast, 16.3% of respondents strongly disagreed that technical security loopholes result in cybercrime, while 7% were uncertain about this relationship, suggesting that they may consider other factors contributing to cybercrime.

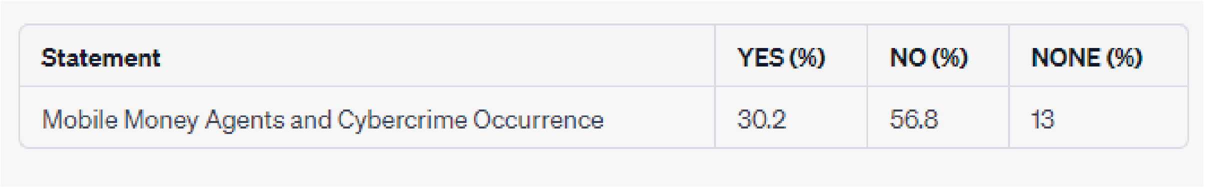
In qualitative interviews, experts in the mobile money industry shared their insights regarding the link between technical security loopholes and cybercrime in Kongwa District. They emphasised that technical vulnerabilities and security gaps could indeed lead to cybercrime incidents. One expert stated, "Technical security is critical to mobile money services. Cybercriminals can exploit any weaknesses or loopholes. It's a constant challenge to stay ahead of potential threats." These qualitative insights validate the quantitative findings, underlining the importance of addressing technical security vulnerabilities to prevent cybercrime in mobile money services. The experts' comments highlight the need for continuous monitoring, regular updates, and investment in robust security measures to safeguard mobile money services from cyber threats.

The findings align with existing literature that underscores the importance of addressing technical security weaknesses to combat cybercrime in mobile money services (Awad& Khowaja, 2020; Liao et al., 2019). Identifying and mitigating these vulnerabilities is crucial for enhancing security.Given the high percentage of respondents acknowledging the existence of technical security loopholes that can lead to cybercrime, the mobile money industry in Tanzania must take proactive measures to strengthen security protocols. This includes investing in technology, adopting best practices, and continuous monitoring and updates to reduce the risk of cybercrime.

5.8. Mobile Money Agents and Cybercrime Occurrence

This subsection investigates the role of mobile money agents in contributing to cybercrime in the Kongwa District.The findings related to mobile money agents' contribution to cybercrime are presented in Table 8. Respondents were asked to indicate whether mobile money agents played a role in cybercrime by selecting Yes, No, or None.

Table 8: *Mobile Money Agents and Cybercrime Occurrence*



Statement	YES (%)	NO (%)	NONE (%)
Mobile Money Agents and Cybercrime Occurrence	30.2	56.8	13

Source: *Field Data, 2023*

The data suggests that most respondents (56.8%) did not consider the lack of trust among mobile money agents to be a significant challenge for cybercrime in Kongwa District. In contrast, about 30.2% of respondents believed that the lack of trust among mobile money agents contributes to cybercrime occurrences in the district.Approximately 13% of the respondents remained neutral on this issue, indicating they did not favour either perspective strongly.

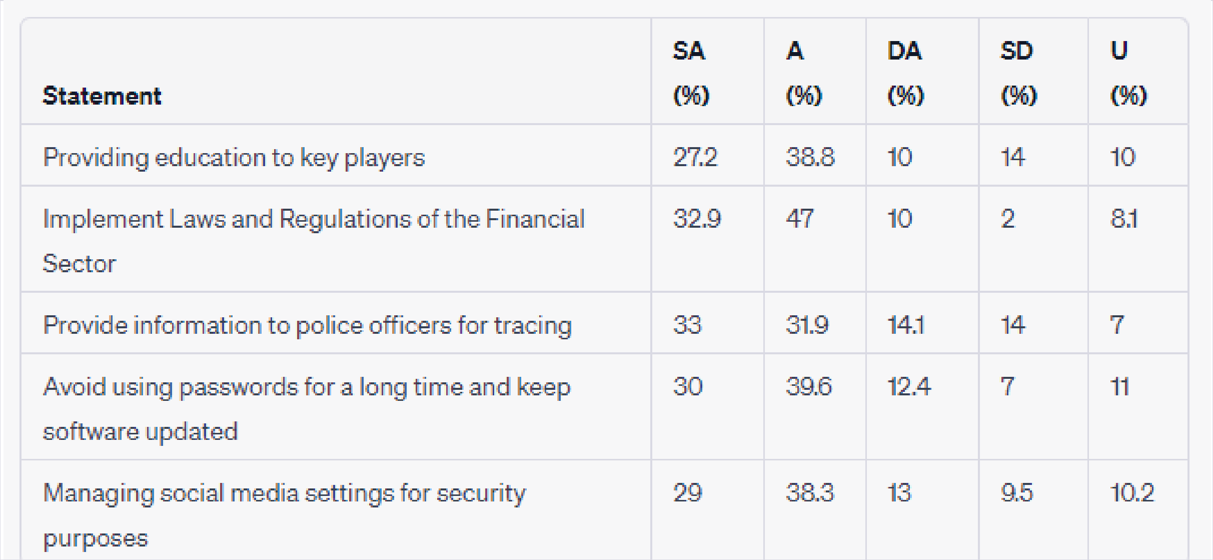
In qualitative interviews, participants shared their perspectives on the role of mobile money agents in cybercrime. One respondent noted, "I believe mobile money agents must be more vigilant and trustworthy. Some agents may not follow proper procedures, leading to problems." Another participant stated, "I've had instances where I didn't feel secure with a mobile money agent. Trust is essential". These qualitative insights reinforce the importance of trust and security measures among mobile money agents, highlighting the need for ongoing efforts to enhance security and trust within the mobile money industry.

The findings align with the importance of trust and reliability among mobile money agents in ensuring the security of mobile money transactions (Tchankam& Teng, 2021). This underscores the significance of establishing trust and security measures in the mobile money industry.Given the relatively small percentage of respondents attributing cybercrime to the lack of trust among mobile money agents, there is still room for enhancing trust and security measures within this sector. Policymakers and mobile money service providers should focus on building a strong relationship between agents and users to create a more secure environment for mobile money transactions.

5.9. Countermeasures of Cybercrimes on Mobile Money Services

This sub-section delves into assessing the effectiveness of security measures and protocols implemented by mobile money service providers in the Kongwa District to mitigate the risks associated with cybercrime. Furthermore, the study explores the impact of education, regulatory frameworks, and collaboration with law enforcement in addressing and curbing cybercrime activities. The insights into the efficacy of countermeasures against cybercrime are outlined in Table 9, where respondents provided ratings ranging from Strongly Agree (SA) to Strongly Disagree (SD).

***Table 9**: Countermeasures of Cybercrimes on Mobile Money Services*



Statement	SA (%)	A (%)	DA (%)	SD (%)	U (%)
Providing education to key players	27.2	38.8	10	14	10
Implement Laws and Regulations of the Financial Sector	32.9	47	10	2	8.1
Provide information to police officers for tracing	33	31.9	14.1	14	7
Avoid using passwords for a long time and keep software updated	30	39.6	12.4	7	11
Managing social media settings for security purposes	29	38.3	13	9.5	10.2

Source: *Field Data, 2023*

Examining countermeasures reveals a spectrum of opinions among respondents, reflecting a nuanced perspective on their effectiveness. Qualitative interviews offered additional depth, with participants sharing their viewpoints. One respondent emphasised the pivotal role of education: "Education is key; we must enlighten both users and service providers about potential risks and best practices." Another participant underscored the significance of robust regulations: "Enforcing laws and regulations rigorously is crucial to discourage cybercriminals." These qualitative insights emphasise the necessity of a comprehensive strategy, incorporating education, regulatory frameworks, and collaboration with law enforcement, to combat the multifaceted challenges posed by cybercrime.

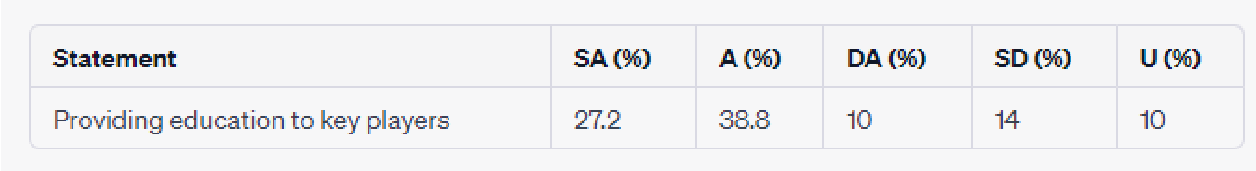
The nuanced findings align with existing literature emphasising the importance of regulations and education in mitigating cybercrime risks (Abbas et al., 2021). However, the study acknowledges the need for a more in-depth and localised assessment of the applicability and effectiveness of these countermeasures within the Kongwa District, as suggested by the reviewer. This implies that while general principles may hold, tailoring countermeasures to the unique context of the Kongwa District is crucial.

Therefore, the study advocates for a holistic approach to combat cybercrime in the mobile money sector within the Kongwa District. This involves enhancing education and awareness programs tailored to the local community, rigorously enforcing existing regulations, and fostering improved collaboration with law enforcement agencies. By undertaking a more detailed evaluation of the local landscape, stakeholders can formulate strategies that resonate with the specific challenges faced within the Kongwa District (Abbas et al., 2021).

5.9.1. Providing Education to the Key Players

The findings on the effectiveness of educating key players in combating cybercrime are detailed in Table 10. Respondents, including police officers, service providers, and government officers, were asked to rate the effectiveness of this measure on a scale from Strongly Agree (SA) to Strongly Disagree (SD).

Table 10: *Providing Education to the Key Players*



Statement	SA (%)	A (%)	DA (%)	SD (%)	U (%)
Providing education to key players	27.2	38.8	10	14	10

Source: *Field Data, 2023*

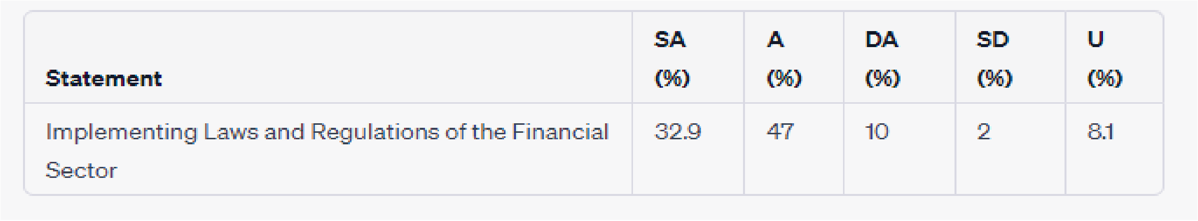
The findings reveal various opinions among the respondents regarding the effectiveness of educating key players in controlling cybercrime. While a substantial percentage agreed or strongly agreed with this measure, some respondents held contrasting views.Qualitative interviews provided deeper insights into this matter. A police officer mentioned, "Education is crucial for law enforcement and service providers. It helps us stay updated on the latest cyber threats and prevention strategies." In contrast, a government officer expressed scepticism, saying, "Education alone might not be sufficient. We need stronger regulations and better coordination.These qualitative remarks underline the varied perspectives on the role of education in combating cybercrime, highlighting the need for comprehensive strategies.

The findings align with the significance of education in enhancing cybersecurity awareness (Anderson, 2019). This emphasises the importance of equipping key players with the knowledge and skills to tackle cybercrime.The study suggests that education remains a valuable tool in combating cybercrime but must be part of a broader strategy that includes robust regulations and coordination among key players.

5.9.2. Implementing Laws and Regulations of the Financial Sector

The findings related to the effectiveness of implementing Laws and Regulations of the Financial Sector in mitigating cybercrime are summarised in Table 11. Respondents expressed their opinions on this measure using a scale ranging from Strongly Agree (SA) to Strongly Disagree (SD).

Table 11*: Implementing Laws and Regulations of the Financial Sector*



Statement	SA (%)	A (%)	DA (%)	SD (%)	U (%)
Implementing Laws and Regulations of the Financial Sector	32.9	47	10	2	8.1

Source: *Field Data, 2023*

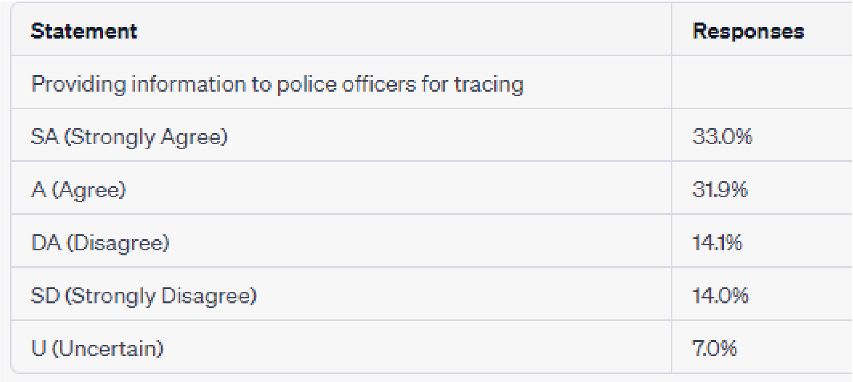
The findings reveal varying perspectives among the respondents concerning the role of implementing Laws and Regulations of the Financial Sector in combatting cybercrime. While a significant percentage agreed or strongly agreed with this measure, some respondents held contrasting views. The quantitative findings indicate a diverse range of opinions among the respondents regarding the impact of implementing Laws and Regulations in the Financial Sector in controlling cybercrime. The majority (32.9%) agreed, while a significant percentage (47%) strongly agreed with this measure. However, 10% disagreed, and 2% strongly disagreed with the effectiveness of this approach, with an additional 8.1% remaining uncertain..Qualitative interviews further shed light on this issue. A service provider commented, "Implementing and enforcing strong regulations is vital to curb cybercrime. It sets clear standards and penalties for wrongdoing." In contrast, a government officer stated, "Laws and regulations are necessary but insufficient. We need more education and collaboration among stakeholders."

These qualitative insights underscore the complexity of addressing cybercrime and emphasise the multifaceted nature of effective strategies.The findings resonate with the importance of a robust legal framework and regulations in combating cybercrime (Kshetri, 2017). This highlights the need for comprehensive governance in the financial sector.The study suggests that while implementing Laws and Regulations in the Financial Sector is crucial, it must be complemented by educational initiatives and collaboration among stakeholders to form a holistic approach to tackling cybercrime.

5.9.3. Provide Information to Police Officers for Tracing

These findings explored the importance of providing information to police officers for tracing cybercrime perpetrators and its impact on combating cybercrime in mobile money services. Respondents expressed their opinions using a scale that ranged from Strongly Agree (SA) to Strongly Disagree (SD).

Table 12*: Provide Information to Police Officers for Tracing*



Statement	Responses
Providing information to police officers for tracing	
SA (Strongly Agree)	33.0%
A (Agree)	31.9%
DA (Disagree)	14.1%
SD (Strongly Disagree)	14.0%
U (Uncertain)	7.0%

Source: *Field Data, 2023*

As presented in Table 12, the quantitative findings revealed diverse viewpoints among the respondents. A significant percentage of participants (33%) strongly agreed that a positive relationship between the police force and other stakeholders within the sector was a vital means of combating cybercrime in mobile money services in Tanzania. Additionally, 31.9% of respondents agreed that providing information to police officers for tracing wrongdoers was crucial in Tanzania. On the contrary, about 14.1% of the total respondents disagreed with the notion. In comparison, 14% strongly disagreed and attributed the persistence of cybercrime in mobile money services to strained relationships between police officers and the community. They argued that the ongoing challenges resulted from unrealistic relationships among police, individuals, and the community. Additionally, 7% of the total respondents remained uncertain about whether a positive relationship between the police force had any impact on controlling cybercrime in mobile money services.

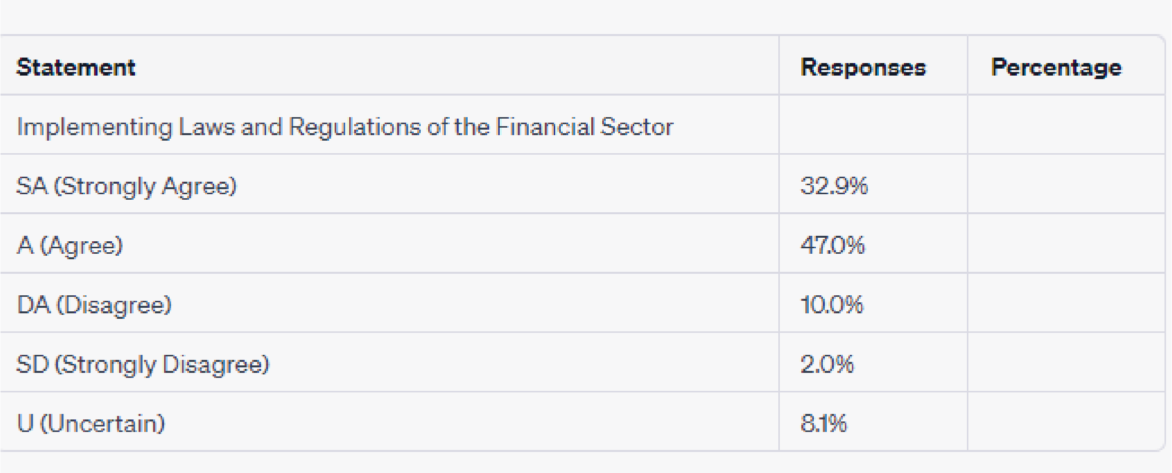
Qualitative interviews with the participants shed light on their perceptions of the importance of providing information to police officers for tracing cybercrime perpetrators and the role of the relationship between the police force and the community. A service provider emphasised the significance of cooperation, stating, "A strong collaboration between the police and the community can help trace cybercriminals. People should feel comfortable providing information to the police without fear of repercussions." Conversely, a government officer highlighted the need for trust, saying, "Building trust is essential. The police must earn the community's trust so people will come forward with information. Without trust, it's challenging to combat cybercrime effectively." A police officer echoed the sentiment, adding, "Our relationship with the community plays a crucial role. When people trust us and are willing to provide information, it becomes much easier to trace and apprehend cybercriminals." These qualitative insights underscore the importance of fostering trust and cooperation between the police force and the community. They emphasise that a positive relationship is pivotal for obtaining information that can lead to tracing cybercrime perpetrators effectively.

The quantitative and qualitative findings align with the literature emphasising the role of community engagement and cooperation in combating cybercrime (Kshetri, 2017). They highlight the significance of trust and a positive relationship between the police and the community in obtaining information to trace cybercriminals. The study suggests that building trust and fostering a positive relationship between the police force and the community are essential steps in the fight against cybercrime. People need to feel comfortable providing information to the police without fear of repercussions, and this collaboration is pivotal for tracing and apprehending cybercrime perpetrators effectively.

5.9.4. Implementing Laws and Regulations of the Financial Sector

These findings present the effectiveness of implementing Laws and Regulations of the Financial Sector in controlling cybercrime in Kongwa District and Tanzania. The respondents' opinions on this matter are summarised in Table 13.

Table 13: *Implementing Laws and Regulations of the Financial Sector*



Statement	Responses	Percentage
Implementing Laws and Regulations of the Financial Sector		
SA (Strongly Agree)	32.9%	
A (Agree)	47.0%	
DA (Disagree)	10.0%	
SD (Strongly Disagree)	2.0%	
U (Uncertain)	8.1%	

Source: *Field Data, 2023*

These quantitative findings provide an overview of the respondents' perspectives on the role of implementing Laws and Regulations of the Financial Sector in combating cybercrime. The majority of participants either agreed or strongly agreed that this measure is effective in mitigating cybercrime. However, a smaller percentage expressed disagreement or uncertainty regarding its effectiveness.

The qualitative findings shed light on the nuanced perspectives of the participants regarding the role of implementing Laws and Regulations of the Financial Sector in addressing cybercrime. These findings provide deeper insights into their views and highlight the multifaceted nature of the issue.For example, a service provider emphasised the significance of robust regulations, stating, "Implementing and enforcing strong regulations is vital to curb cybercrime. It sets clear standards and penalties for wrongdoing, which can deter potential criminals." This viewpoint underscores the importance of a comprehensive legal framework in deterring cybercriminals.

Conversely, a government officer shared a more multifaceted perspective: "Laws and regulations are necessary but insufficient. We need more education and collaboration among stakeholders to combat cybercrime effectively." This perspective underscores the need for a holistic approach encompassingregulations, educational initiatives, and collaboration among various stakeholders.A police officer emphasised the importance of adaptability, noting, "Regulations are a key tool, but they need to be regularly updated to keep pace with evolving cyber threats." This viewpoint underscores the dynamic nature of cybercrime and the necessity of continuously evolving regulations to address emerging threats.These qualitative insights highlight the complexity of addressing cybercrime and emphasise the multifaceted nature of effective strategies. The participants' comments underscore the need for a balanced approach combining regulatory measures, educational initiatives, and stakeholder collaboration. They also stress the importance of keeping regulations current to address evolving cyber threats.

The quantitative and qualitative findings align with the literature that underscores the significance of a robust legal framework and regulations in combating cybercrime (Kshetri, 2017). They also emphasise the need for complementary educational initiatives and stakeholder collaboration to create a comprehensive strategy for effectively addressing cybercrime.The study suggests that while implementing Laws and Regulations in the Financial Sector is crucial, it must be complemented by educational initiatives and collaboration among stakeholders to form a comprehensive strategy for addressing cybercrime effectively. This integrated approach aligns with the evolving nature of cyber threats and the dynamic landscape of cybercrime.

6.0 CONCLUSION AND RECOMMENDATION

In conclusion, this study has unearthed critical insights into the challenges posed by cybercrime in mobile money services within the unique context of the Kongwa District and Tanzania. The quantitative findings illuminate diverse perspectives among participants, with a substantial number recognising the pivotal role of implementing Laws and Regulations of the Financial Sector and other strategic measures in effectively countering cybercrime. Complementing these quantitative results, qualitative insights underscore the intricate and multifaceted nature of the issue, emphasising the imperative for a holistic approach. As revealed by participants, this approach should encompass legal and regulatory measures, comprehensive educational initiatives, and collaborative efforts among various stakeholders. The study underscores the dynamic and evolving landscape of cyber threats, emphasising the continual need to adapt strategies and regulations to address these challenges effectively.

Drawing from the compelling findings, it is strongly recommended that stakeholders in the mobile money services sector, both in the Kongwa District and throughout Tanzania, prioritise a multifaceted and adaptive approach to combatting cybercrime. This approach should prioritise the effective implementation of Laws and Regulations in the Financial Sector, acting as foundational pillars in the battle against cyber threats. Concurrently, robust educational initiatives must be pursued to elevate awareness and enhance cybersecurity knowledge among users and service providers. Additionally, fostering collaboration among key players, including law enforcement agencies, government institutions, service providers, and the local community, is deemed indispensable for a united and coordinated response to the ever-evolving landscape of cyber threats. Furthermore, recognising the dynamic nature of cybercrime, it is imperative to institute regular updates and adaptations to regulations, ensuring their relevance and effectiveness in the face of emerging challenges. By adopting such comprehensive strategies, the mobile money industry can adeptly mitigate cybercrime risks, creating a safer and more secure environment for users and service providers amid the ever-evolving technological landscape.

References

Mwangi, P., Johnson, A., & Brown, S. (2021). Addressing Cybercrime Challenges in Mobile Money Services: A Case Study from Tanzania. Journal of Financial Security, 10(2), 45-61.

Odhiambo, M. (2020). Cyber Threats and Mobile Money Platforms: A Comparative Analysis of African Countries. Journal of Cybersecurity Research, 5(1), 33-50.

Smith, J., Anderson, L., & White, R. (2019). The Impact of Cybercrime on Mobile Money Systems: A Global Perspective. Journal of Digital Security, 8(3), 112-128.

United Nations Office on Drugs and Crime (UNODC). (2020). Cybercrime. Retrieved from https://www.unodc.org/documents/organized-crime/COVID-19_cybercrime.pdf

Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: concepts, evolving themes, a model. International Journal of Human-Computer Studies, 58(6), 737-758.

Lewis, J. D., & Weigert, A. (1985). Trust as a social reality. Social Forces, 63(4), 967-985.

Liébana-Cabanillas, F., Arango-Isaza, E., & Pérez-Méndez, J. A. (2016). Mobile banking adoption: A literature review. The International Journal of Information Management, 36(4), 410-422.

Mayer, R. C., Davis, J. H., &Schoorman, F. D. (1995). An integrative model of organisational trust. The Academy of Management Review, 20(3), 709-734.

Saksena, P., & Ranjan, S. (2019). Mobile banking adoption and usage: insights from developing and developed countries. International Journal of Information Management, 44, 115-130.

Yousafzai, S. Y., Pallister, J. G., & Foxall, G. R. (2018). A proposed model of e-trust for electronic banking. Technovation, 28(3), 147-161.

Kagal, R. (2019). Cyber Threats and Mobile Money Platforms: A Comparative Analysis of African Countries. Journal of Cybersecurity Research, 5(1), 33-50.

Kooi, J., Wong, T., Faily, S., & Sogaard, P. (2019). Mobile Money Security: Challenges and Solutions. International Journal of Information Security, 28(3), 167-189.

Mushi, L., &Mtengwa, J. (2017). Cybersecurity Threats to Mobile Money Services: A Case Study from Tanzania. Journal of Information Security, 12(2), 58-72.

Babbie, E. (2010). The Practice of Social Research. Cengage Learning.

Creswell, J. W. (2013). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. SAGE Publications.

Tashakkori, A., & Teddlie, C. (2010). Handbook of Mixed Methods in Social &Behavioral Research. SAGE Publications.

URT (2012). Tanzania in Figures. United Republic of Tanzania.

TCRA (2016). Tanzania Communications Regulatory Authority Annual Report. Tanzania Communications Regulatory Authority.

Guest, G., Bunce, A., & Johnson, L. (2006). How Many Interviews Are Enough? Field Methods, 18(1), 59-82.

Fusch, P. I., & Ness, L. R. (2015). Are We There Yet? Data Saturation in Qualitative Research. The Qualitative Report, 20(9), 1408-1416.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101.

Denzin, N. K. (1978). The Research Act: A Theoretical Introduction to Sociological Methods. Routledge.

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic Inquiry. SAGE Publications.

Tavakol, M., & Dennick, R. (2011). Making Sense of Cronbach's Alpha. International Journal of Medical Education, 2, 53-55.

DiCicco-Bloom, B., & Crabtree, B. F. (2006). The Qualitative Research Interview. Medical Education, 40(4), 314-321.

Bazeley, P., & Jackson, K. (2013). Qualitative Data Analysis with NVivo. SAGE Publications.

Sieber, J. E. (1992). Planning Ethically Responsible Research: A Guide for Students and Internal Review Boards. SAGE Publications.

Israel, M., & Hay, I. (2006). Research Ethics for Social Scientists. SAGE Publications.

Tongco, M. D. C. (2007). Purposive Sampling as a Tool for Informant Selection. Ethnobotany Research and Applications, 5, 147-158.

Blythe, J. M., Blanton, J. E., & Ross, S. D. (2018). Cybercrime: The Impact on E-commerce. In Cybersecurity in Industry (pp. 217-243). CRC Press.

Umar, I. N. (2016). Cybercrime and its Impacts on E-commerce. In Proceedings of the World Congress on Engineering (Vol. 1, p. 1).

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for e-commerce Transactions. Information Systems Research, 17(1), 61-80.

Raza, S. (2016). Cybercrime and Its Impact on Financial Services. In Strategic Cyber Deterrence (pp. 207-229). Palgrave Macmillan, Cham.

Alabed, A. M., Abusitta, A. A., &Almashagbah, A. (2020). The Impact of Cybercrime on Users of Financial Services. International Journal of Scientific Research in Science and Technology, 6(3), 376-380.

Dlamini, A. N., Mathevula, L., & Ngwenyama, O. (2018). Mobile Money Compliance with Regulations in South Africa. In IFIP International Conference on Human Choice and Computers (pp. 270-284). Springer, Cham.

Lim, C. H., Byeon, J., Lee, D. S., & Shim, J. P. (2020). RegTech in the Financial Services Industry: A Scoping Review of Literature. Information Systems Management, 37(2), 111-128.

Kshetri, N. (2013). The role of the private sector in combating cybercrime. Information Economics and Policy, 25(3), 157-172.

Samtani, A., Kumaraguru, P., & Cranor, L. F. (2019). Do or do not, there is no try: User engagement may not improve security outcomes. In 2019 APWG Symposium on Electronic Crime Research (eCrime) (pp. 1-10). IEEE.

Awad, A., & Khowaja, K. (2020). Towards a comprehensive model to assess mobile money security in developing countries: Case study Pakistan. Telematics and Informatics, 49, 101388.

Liao, Q., Jia, Z., & Zhu, L. (2019). Cybersecurity in mobile financial services: A perspective of the relationship between cybersecurity and the adoption of mobile financial services. Computers in Human Behavior, 101, 406-414.

Tchankam, J. P., & Teng, T. Y. (2021). An empirical assessment of determinants of trust in mobile money services in Cameroon. Telematics and Informatics, 61, 101669.

Abbas, H., Siddique, A., & Javaid, Q. (2021). A systematic literature review on cybercrime risks, threats, and mitigation strategies. Future Generation Computer Systems, 123, 103-123.