INVESTIGATION INTO THE RISKS FACING MOBILE BANKING: A CASE OF COMMERCIAL BANKS IN KENYA

BY

JOHN NJAU KARANJA

UNITED STATES INTERNATIONAL UNIVERSITY-AFRICA

SPRING 2017

INVESTIGATION INTO THE RISKS FACING MOBILE BANKING: A CASE OF COMMERCIAL BANKS IN KENYA

BY

JOHN NJAU KARANJA

UNITED STATES INTERNATIONAL UNIVERSITY-AFRICA

A Project Report Submitted to the Chandaria School of Business in Partial Fulfillment of the Requirement for the Degree of Master of Business Administration (MBA)

SPRING 2017

STUDENT'S DECLARATION

I, the undersigned, declare that this is my original work and has not been submitted to any other college, institution or university other than the United States International University-Africa for academic credit.

Signed: _____ Date: ___ _____

John Njau Karanja (ID:628304)

This research proposal has been presented for examination with my approval as the appointed supervisor.

Signed: _____ Date: _____

Dr. Amos Njuguna

Signed: _____ Date:_____

Dean, Chandaria School of Business

ABSTRACT

The objective of the study was to investigate the risks facing mobile banking among the commercial banks in Kenya. The study seeks to answer three research questions. What risks arise for commercial banks in Kenya as a result of mobile banking? What measures are adopted by commercial banks in Kenya to protect against future mobile banking risks? What strategies do Kenyan banks employ to mitigate mobile banking risks?

The current study adopted a descriptive research design. The design was appropriate for the current study since the study sought to express the situation exactly the way it is in the industry. The current study population consisted of 41 informational technology managers in each of the 41 commercial banks registered in Kenya as at 30th June 2016. However, only 37 response resulting into a 90% response rate.

With regard to the first objective the study sought to determine risks arising as a result of malware and majority of the respondents agreed that there were no reported risks arising from malware virus attack on the mobile banking platform. In addition, majority of the respondents agreed that to some little extent of system hacking on radical programmers who steal mobile banking PINs and codes, hackers who secretly read the organization emails. Other issue was unauthorized access by former colleagues and unauthorized persons gaining access to mobile banking systems when the users carelessly leaves their computers it logged on and theft in order to impersonate the customer for accessing mobile banking services.

The second objective established that challenges arising because of security and to some little extent security on third party intrusion, loss of privacy. Majority of the respondents agreed that to some moderate extent availability of alternative, mobile phone access and cost of service is a challenge exhibited. Respondents also agreed that there is limited social factors on customers trust, and limited extent of embracing new technology and awareness. The third objective established that there is a great use of one time SMS verification codes together with the normal PIN. Moreover, respondents agreed that there is little extent use of one time phone call verification codes together with the normal PIN, use of random numbers together with the normal PIN and use of card readers codes together with the normal PIN. To analyse level of encryption by commercial banks majority of the respondents agreed that a great extent there is use of data encryption to achieve a high level of security.

The study concluded that commercial banks have maintained their technology thus ensuring risks related to malware are continuously avoided. There are however risks in regard to system hacking by radical programmers as well as unauthorized access in banks. In addition, the continuous competition in the sector has also contributed to availability of alternative services, mobile phone access and related cost of service. There is a continued use of one time SMS verification codes together with the normal PIN. Moreover, respondents also enjoy one time phone call verification codes together with the normal PIN, use of random numbers together with the normal PIN and use of card readers codes together with the normal PIN. The banks also use data encryption to achieve a high level of security and use of data encryption also help avoid misuse of data.

The study recommended that the commercial banks need to maintain their technology to ensure the related malware risks are continuously avoided. There also a need to beef up the set up ensure cases of system hacking by radical programmers. The commercial banks need to analyze security and set up stringent measures to curb cases of third party intrusion, and loss of privacy. In addition, there is a need to inform the customers of the benefits associated with use of mobile banking service. It was also concluded that Banks need to enhance their use of one time SMS verification codes together with the normal PIN. The firms also need to continuously adopt PIN related features and use of data encryption to achieve a high level of security and avoid misuse of data. There is a need to undertake further studies to establish the effects of the risks established on the profitability of commercial banks in Kenya.

COPYRIGHT

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my supervisor Dr. Amos Njuguna for his dedication and time that has enabled me successfully complete this research report, I am forever grateful.

DEDICATION

This report is a special tribute and dedication to my late parents Julius Njau Mwihia and Martha Njeri Njau who passed on when I was undertaking my Master's degree. You will always be in a special part in our hearts.

TABLE OF CONTENTS

LIST OF TABLES

ACRONYMS AND ABBREVIATIONS

CAK: Communications Authority of Kenya

CBK: Central Bank of Kenya

FSD: Financial Sector Deepening

GDP: Gross Domestic Product

GSMA Global System Mobile Association

ISACA: Information Systems Audit and Control Association

KPMG: Klynveld Peat Marwick Goerdeler

MEF: Mobile Ecosystem Forum

SD: Standard Deviation

TLS: Transport Layer Security

CHAPTER ONE

1.0 INTRODUCTION

1.1 Background of the Study

Innovation plays a pivotal role in the growth and survival of companies, especially in dynamic and complex markets with uncertain economic circumstances (Cheng, Lee, & Lee, 2014). Mobile technology has emerged as one of the most malleable form of innovation in the last 30 years. The technology provides organizations with multiple platforms for achieving various organizational operations efficiently and effectively. The mobile technology was primarily developed as a voice communication system but with time, mobile phones have evolved to incorporate applications used in machine automation, e-Government services, mobile banking services among others (AlSoufi & Ali, 2014). In fact, the technology has been at the center stage of business operations' revolution.

In the banking sector, Mahad, Mohtar, Yusoff and Othman (2015)assert that the mobile technology has played a critical role in enhancing efficiency, access and convinience to the users. The use of mobile technology in the banking sector has moved from mere non-transactional tasks such as checking of account balances, viewing of recent account transactions and downloading of bank statements in the early 2000s to more complex transactional task such as funds transfer, bill payments, investment purchase or sale, loan applications and transactions, shoping, donationsamong others (Priya & Raj, 2015).Joubert and Belle (2013) assert that the rapid development in mobile communication technologies and its high penetration persents an opportunity for growth in the banking sector especially in the developing countries where computer-based internet access is very low.

Globally, rapid growth and adoption of smartphone use has become the principal axis for the expansion of mobile banking. According to the Global Mobile Money report 2015, 69% of mobile device users globally carried out banking activities via their mobile phones in 2015(MEF, 2016). This is huge considering that worldwide mobile phone penetration stood at 96% in the year 2015 (Mahad, Mohtar, Yusoff, & Othman, 2015). Further, the number of mobile banking users globally is projected to grow by more than 125% by 2019 (KPMG, 2016).

In Africa, the 2016 report published by GSMA Intelligence on Africa's mobile economy indicates that at the end of 2015, 46%of the population (more than half a billion people) in Africa subscribed to mobile phone services (GSMA, 2016). The report further shows that in 2015, the number of mobile device uses in Africa who carried out financial transactions on their mobile gargets averaged 80% (MEF, 2016). Moreover, the mobile technologies, and services generated 6.7% of Africa's GDP and3.8 million jobs in 2015(GSMA, 2016).

In Kenya, according to the Communication Authority of Kenya (CAK), mobile penetration stood at 88.1% (37.8 million subscribers) by the end of September 2015. The data market registered 21.6 million subscriptions, with the number of internet users growing to 31.9 million and the mobile money transfer service subscriptions growing to 28.7 million (74.2%) (CAK, 2015). Data from the Central Bank of Kenya (CBK) indicates that Ksh. 3.087 trillion was transacted through the mobile phone platform in the 2015/2016financial year (CBK, 2016). Out of these transactions, person-to-person transfers stood at 64.7% and mobile commerce at 35.2%. The total money transferred via the mobile platform in 2015 in Kenya was equivalent to 48.6% of the Country's GDP.

Mobile banking is the provision and execution of banking and financial services through the help of mobile telecommunication device ssuch as the telephone or tablets (Okiro & Ndungu, 2013). According to a report by FSD Kenya (2016), 80% of the Kenyan banks in partnership with the major telecommunication companies (Safaricom, Orange, Essar, and Airtel) offer mobile banking solutions to their clients. Moreover, the telecommunication companies on their own also provide financial services such as M-pesa by Safaricom, Orange money by Orange, Yu-cash by Essar, and Airtel money by Airtel.The platforms facilitate real-time payments, mobile savings and loans service, stock market transactions, accounts administrations, and access to customized information (Okiro & Ndungu, 2013).

Despite the potential of the mobile banking in enhancing financial inclusion, reducing the cost of banking and increasing convenience (Opili & Muturi, 2016), a study by He, Tian andShen (2015) observes that mobile banking security threats have been increasing in frequency and sophistication in the last 10 years. The study links the threats to a variety of damages and criminal activities including leaking of sensitive financial data, economic loss, identify theft and fraud.

Therefore, mobile banking security threats have become a major concern to the financial service providers and their clients. A study by Heggestuen (2014)in the United States of America showed that 31% of mobile banking clients demonstrated that they would be willing to spend more or absorb more charges just to make sure that their mobile transactions are secure. Further, 63% would consider more secure mobile banking platforms if a breach is detected in their current mobile banking platforms. Moreover, the study established that 71% of mobile banking clients would consider switching accounts to accounts that guaranteed that losses from mobile security breaches would be reimbursed.

A study by Webroot (2014) observed that compared to other online platforms, mobile phones have greater security risk. The study attributed the risk to less user authentication; more focus on convenience instead of security; easier access to data on compromised mobile phones; ease of account and document access via email; unsafe data transmission over unsecured wireless connections; sensitive data leakage due to poor app coding; and unsafe data storage as mobile applications often save sensitive data, such as banking authentication codes. Research shows that these risks have become more frequent due to inadequacies in technical skills for combating cybercrime; weak legislations; availability of a variety of mobile phone platforms; and the faster rate at which the attacks take different forms (He, Tian, & Shen, 2015).

Due to this, concerted efforts have been put forward in identifying and fighting cybercrime worldwide. Islam (2014) conducted a comprehensive systemic literature review on security challenges of mobile phone banking between 2008 and 2012 in Malasyia and observed that unauthorised access, malicious hacking, malware and and mobile viruses were the most significant threats during that period. A study by He, Tian and Shen (2015) recommends an innovative account profiling technology; biometric based authentication and identification systems; Transport Layer Security (TLS) protocol combined with a proposed trust negotiation method; and encryptions as some of the strategies for adressing the mobile banking security threats. However, the study did not show empirical evidence for the same.

Being a recent platform that is highly dynamic, there is need to fully understand the ever changing faces of the mobile banking security threats and how the risks can be mitigated. Studies carried out on mobile bankingdo not clearly expose the current risks faced by

commercial banks in Kenya. This research seeks to establish the previaling risks of mobilebanking and strategies adopted by commercial banks in Kenya to mitigate the risks. Itaims at providing information that can help inincrease mobile banking security and safeguard against customer and bank losses for enhanced organizational performance.

According to the Central Bank of Kenya (2016) as at June 2016, there were 62 commercial banks in Kenya. Twenty-five of these banks were locally controlled (>50% local ownership); while 15 were foreign controlled (>50% foreign ownership) and three where government controlled (>50% government ownership). This sector plays a critical role in the Kenyan economy contributing upward of 22% of the GDP (IFC, 2016). The current study was a census of all the 62 commercial banks in Kenya.

1.2 Problem Statement

Mobile banking technology has been widely adopted by commercial banks in Kenya as a strategic tool for market penetration, without massive investment in physical infrastructure. The technology has been very instrumental in serving a wide and ever-growing customer base with fast, efficient, and convenient quality services (Kombe & Wafula, 2015). Mobile banking has therefore become one of the key success factors in the banking industry as empirical evidence links its adoption to wide customer base and enhanced number of transactions. However, risks associated with mobile banking has generated considerable interest for the service providers as well as their clients (Simpson, 2002).

Several studies have been conducted on the concept of mobile banking risk. However, as argued by Islam(2014) the concerns for mobile banking risks in most cases are fears born more of perception than reality. Despite existence of some of these threats, there are security controls, which affectively and substantially mitigate their risk. Thus, some perceived threats do not always constitute significant risks. Moreover, security practices and threats are continuously evolving as mobile technology advances. This creates an ever-growing demand for understanding the significant prevailing and potential mobile banking security risks in given contexts.

In the USA, a study by ISACA (2011) showed denial of service, theft of services, message modification, theft of content, digital piracy,digital rightsinfringement, loss of revenue and illegal transfer of funds as the main risks facing mobile banking service

providers. In Africa, a study by Masamila (2014) to explore the state of mobile banking and its associated threats in Tanzania identified viruses and malwares, which can potentially lead to eavesdropping on user activities, stealing of sensitive information, destruction of stored information, deactivation or activation of applications or disablement of a device as the main security concerns for firms that provide mobile banking. In Kenya, a study by Rosen (2013) to evaluate mobile banking identified system failure as the main risk facing mobile banking service providers. The variations in the findings show how dynamic, diverse, and context based the risks for mobile banking can be. Hence, there is need for clarity on the actual and prevailing mobile banking risks facing the service providers in different contexts.

Despite these studies offering a rich information base on the mobile banking risks, there is scarcity of empirical evidence about the prevailing security risks facing mobile banking in commercial banks in Kenya. This denies the banks valuable information for conducting cost benefit analysis for adopting the technology. This study therefore seeks to fill this knowledge gap by examining the current risks facing mobile banking among the commercial banks in Kenya

1.3 Purpose of the Study

To investigate the risks facing mobile banking among the commercial banks in Kenya.

1.4 Research Questions

1.4.1 What risks arise for commercial banks in Kenya because of mobile banking?
1.4.2 What challenges arise for commercial banks because of mobile banking?
1.4.3 What strategies do Kenyan banks employ to mitigate mobile banking risks?

1.5 Significance of the Study

1.5.1 Management of Financial Institutions

The findings will be significant to the management of financial institutions in Kenya. The study intends to highlight the risks. This information will be critical in reevaluating and redesigning the mobile banking systems to achieve a reduction on the risks and enhance organizational performance.

1.5.2 Policy Makers

Insights from this study will be crucial in directing policy in mobile telephony. The information may be critical in formulating legislations that protect users from mobile banking risks and fraud.

1.5.3 Researchers

Literature review identified inadequacies of knowledge on prevailing mobile banking security risks of the commercial banks in Kenya. Findings from this study will provide the needed empirical evidence to draw conclusion on the subject.

1.6 Scope of the Study

The study focused on evaluating the mobile banking risks for commercial banks in Kenya. The study will explore the risks, and measures taken by the commercial banks in mitigating the existing and potential future risks. The population of the study comprised of the 62 commercial banks in Kenya. Data collection for the study was done between the months of November and December 2016.

1.7 Definition of Terms

1.7.1 Risk

Possibility of loss or something unpleasant happening because of use or association with a given technology or item.

1.7.2 Commercial Banks

Financial institutions, which provide services such as accepting deposits, making business loans, and offering basic investment products.

1.7.3Mobile Banking

Mobile banking defines the provision and execution of banking and financial services through the help of mobile telecommunication devices such as the telephone or tablets (Okiro & Ndungu, 2013).

1.8 Chapter Summary

The chapter laid down the basis for the study. It gave the study background and established the knowledge gap, and presented the objectives of the study. The Chapter further presented the significance of the study, scope of the study and the definition of terms. Chapter Two will be a review of literature, while chapter three will offer the

methodology to be followed to actualize the study objectives. Chapter Four will give the findings and finally Chapter five will offer the discussions and recommendations from the study.

CHAPTER TWO

2.0 LITERATURE REVIEW

2.1 Introduction

This chapter reviews both empirical and theoretical literature on the subject matter. The first section explores mobile banking risks. The second section discusses measures adopted to protect against future risks while the third section covers strategies for dealing with the current risks.

2.2 Mobile Banking Risks

2.2.1 Malwares

A malware is any type or form of computer based software intended to gain access to a computer systems or networks with the aim of disturbing computer operations or gathering personal information without taking the consent of system's owner (Gandotra, Bansal, & Sofat, 2014). Therefore, they are programs that intentionally exploit vulnerabilities in computing systems for a harmful purpose (Elhadi, Maarof, & Barry, 2013). He, Tian and Shen (2015) write that with increased usage of mobile banking, mobile malware has been increasing in frequency and sophistication. This has caused a lot damages including leaking of sensitive financial data, financial loss and identify theft.

To put the threat of malwares into perspective, more than 100,000 new malware samples are recorded every day (FSEC Global, 2016). This means that every second, a new malware variant is being released. First quarter of 2016 report by McAfee Labs on the state of malwares indicated that there is an enomous increase in cases where cybercriminals use malwares to exfiltratie user data, inspect files, send fake SMS messages, load additional apps without user consent, and send user location information to control servers. These were reported in more than 5,000 versions of 21 applications designed to provide useful user services such as mobile banking, health monitoring, and travel planning(McAfee Labs, 2016).

According to Elhadi, Maarof and Barry (2013) malwares can be differentiated based on whether the software needs or does not need a host program to function; or whether the software produces copies of itself or not. Malwares therefore include computer viruses which try to replicate themselves into other executable codes. There are also trojan horses which are computer programs that are benign and have useful functions however, they

have hidden potentialmalicious functions that avoid system security measures. Third are worms that self-replicates and disseminates versions of itself across a network (Elhadi et. al, 2013).

Other malwares included backdoors which present secret entry points into a program that allow someone who is aware of its existence to gain unauthorized access to the system without going through the normal security check. Further, there are spywares which gather information from a victim's computer and sends it to the spyware creator. There are also tootkits which enable root-level access; and botnets which are activated by a certain trigger on a machine to attack and infect other machines (Elhadi et. al, 2013).The current study presumes that with the increase in adoption of mobile banking across banks in Kenya, the new generation malwares present a risk to the banks.

2.2.2 System Hacking

Unlike malwares where the program is released to collect information or interfere with computer operations, hacking requires an active involvement of a human being. In simpler terms, malwares are designed to act on behalf of the creator while hackers directly modify or interfere with a computer system. Hence, Farsole, Kashikar and Zunzunwala (2010) define hackers as a person who like to tinker with software or electronic systems. That is, a radical programmer who aggressively explores creative solutions to problems. These programmers may use their talents to subvert criminal activities or for malicious and illegal purposes (Falk, 2014).

Major concerns are on hackers who use their talents for malicious intent. Farsole, et al. (2010) posit that organizations are particularly afraid of hackers who break into web servers to replace their logos with pornography, read their e-mails, steal credit card numbers from an on-line shopping site, or implant software that will secretly transmit the organization 's secrets to software that will secretly transmit their organization 's secrets to the open Internet.

According to Pujitha and Mallu (2013), due to increase in use of mobile banking, chances of mobile hacking for financial benefits have heavily increased with over-the-air mobile data hacking in network path from bank to customer mobile handset including MPIN being the major concern. This has been made grave by the fact that hackers have the ability to steal bank information using various techniques in duping mobile phone users to believe that they are communicating with a genuine program from the bank while in

reality the user is giving away sensitive information to the hackers (Luvanda, Kimani, & Kimwele, 2014).

2.2.3 Unauthorized Access

The distinction between hacking and unauthorized access is that the latter involves gaining access to a computer system by improper means while unauthorized access describes gaining access to a computer system using usual means of access but without consent (Morgan, 2015). Unauthorized access includes gaining access to some else's authentication code and using it to access a system or simply gaining access to a computer system when the user carelessly leaves it logged on. This has mainly been attributed to customers' widespread use of static passwords which can be guessed, forgotten, written down and stolen, or eavesdropped (Hayikader, Hadi & Ibrahim, 2016).

Customers are particularly worried of their accounts being accessed through their personal account details by way of stolen PIN codes (Mahad, Mohtar, & Othman, 2016). Unauthorized access may also be presented through identity theft where key pieces of someone's identifying information is acquired through theft in order to impersonate them and commit various crimes in that person's name (Information and Privacy Commissioner (IPC), 2014). According to Webroot (2014), mobile devices present greater opportunity for identity thieves due to less user authentication during data sharing; more focus on user convenience over user security; easier access to data on compromised mobile devices; ease of account and documentaccess via email or cloud storage; unsafe data transmission over wireless connections and unsecuredpublic Wi-Fi; unsafe data storage of banking PINs, card numbers, and passwords; and data leakage due to poor app coding or authentication that exposes sensitive data to third parties.

Several strategies have been proposed to deal with authorized access when conducting sensitive transactions on mobile devices. Such is the two-factor authentication which require at least two different "factors" before being granted access (Hayikader, Hadi & Ibrahim, 2016). The other methods include one-time passwords used by customers; use of phone or SMS authentication codes; session timeouts after some time; automatic lockouts after set unsuccessful attempts; creation of strong passwords suggested and assisted on by the platform (Musaev & Yousoof, 2015).

2.2.4 Mobile Fraud

The term fraud has drawn varied definitions. Sharma and Panigrahi (2012) posit that fraud entails wrongful or criminal deception intended to result in financial or personal gain. Phua, Lee, Smith and Gayler (2005) defined fraud as any activity that leads to the abuse of a profit organization's system without necessarily leading to direct legal consequences. However, Wang, Liao, Tsai and Hung (2006) expanded the definition to mean deliberate acts that are contrary to law, rule, or policy with intent to obtain unauthorized financial benefit and intentional misstatements or omission of amount by deceiving users of financial statement.

The distinction between mobile frauds from the threats is in the purpose of the act. Mobile banking fraud is expressly concerned with financial deceptions and losses. Therefore, Mudiri, (2012) defines mobile banking fraud in the context of mobile money as the intentional and deliberate action undertaken by players in the mobile financial services ecosystem aimed at deriving gain in cash or e-money, and/or denying other players revenue and/or damaging the reputation of the other stakeholders.

Mobile banking can originate from a number of sources. The fraud may be driven by the consumer, agents, business partners, system administrators or mobile financial service providers. As indicated by Hoffmann and Birnbrich (2012) mobile banking fraud hurts more than just the financial position of both the banks and their customers. For example, Gates and Jacob (2009) posit that as the banks incur substantial operating costs by refunding customers' monetary losses, bank customers experience considerable time and emotional losses as they have to detect the fraudulent transactions, communicate them to their banks, initiate the blocking and re-issuance or re-opening of accounts, and dispute the reimbursement of their monetary losses (Hoffmann & Birnbrich, 2012).

Mobile banking fraud further erodes customer perception, trust and confidence in the bank products. Thus, mobile banking fraud may damage the bank-customer relationship. It may also increase customer dissatisfaction, which may negatively affect customer loyalty and stimulate switching behavior, thereby hurting the banks' reputation and impeding the attraction of new customers (Hoffmann & Birnbrich, 2012). This then influences the banks financial bottom lines.

2.3 Challenges of Mobile Banking

New technology and innovation is believed to present risk for many customers, hence they react differently based on their innate characteristics, the wants and the needs of their companies and the behavior of other buyers. Adoption of innovation therefore depends on relative advantage, compatibility, complexity, triability and observability of the innovation (Rogers, 2013). There are several other factors which have been identified by various researchers as affecting mobile banking adoption and they can be categorized into security, economic, social and infrastructure factors. Donner and Tellez (2008) have given

examples of social and economic factors which influence the dynamics of mobile banking and affect technology adoption. Some of the social factors include conceptualizing electronic money, the social context of transactions, awareness, attitude towards change (embracing new technology), trust in one's bank or service provider, convenience of the service and the comfort that people have in using these services. Economic factors include mobile phone access, cost of the service and availability of alternatives. Infrastructure factors include service availability and reliability, ease of use, network coverage, handset operability and availability of the service on different mobile networks. Other factors fronted propose that mobile banking usage patterns appear to be largely driven by personal missions and marketing strategies of service providers (Njenga, 2011)

2.3.1 Security

Security is the biggest challenge facing the mobile banking world. The use of wireless technology creates a risk that information will be stolen, therefore service providers have to employ the use of highly secure encryption technology to prevent third party data intrusion and losses. Venable Telecommunications (2008) argue that the ubiquitous tools of mobile banking open the door to enormous potential for monetary as well as reputation risk, hence mobile banking service providers have to provide security which is commensurate with the size of the financial institution as well as the complexity of the products and services offered. The mobility of the mobile handset and the nature of wireless communications make it difficult to authenticate a customer, hence this becomes a security concern as well for both the banks and their customers.

Ochuma (2007) laments that the major concern in mobile banking is security and banks and vendors need to address this issue more urgently. He argues that the requirement that a customer needs to transact is personal identification number (PIN)which does not guarantee that the person transacting is the real card holder. Security and privacy issues are the most complicated challenges that need to bead dressed jointly by mobile application developers, wireless network service providers and the banks' IT departments to make users feel more comfortable thereby increasing adoption levels (Venable Telecommunications, 2008).

Consumers' perception of insecurity has been continuously mentioned as the key deterrent against the adoption of mobile banking. A survey conducted by the Federal Reserve determined that 48% of respondents cited concerns about security as their main reason for not using mobile banking. Additionally, 32% of the respondents rated the security of mobile banking for protecting their personal information as somewhat unsafe and very unsafe, whereas 34% were not sure of the security. (Consumer and Mobile Financial Services, 2012). Pegueros (2012) argues that customers' perceptions may not necessarily be irrational when you analyze the security risks of mobile banking. She asserts that the relative immaturity of mobile banking brings many inherent risks in the areas of new technologies, new inexperienced entrants in the field and the complex nature of the supply chain. A majority of these new entrants may be innovative and dynamic but have minimal experience or attention to the area of security. Mobile application development, mobile hosting and personal privacy are some of the areas that are prone to the highest risk.

Pegueros (2012), further observes that the security risks associated with mobile devices are very similar to those evident in any other computing device with a few key exceptions namely: that mobile devices have a smaller form factor and therefore are more susceptible to loss or theft; secondly, mobile devices are more personal and there will be a tendency for users to use devices in a more personal and confidential way, and; lastly, the security controls and tools available have not matured to accommodate the constraints of limited processing power and limited battery life.

A study conducted by Luvanda *et al* (2014) on Kenyan mobile phone users determined that the majority were more interested with the ease at which they could use their phones to perform financial transactions rather than with the related security issues, in total

disregard of the evident manifestation of the latter. The researchers asserted that the increased use of mobile phones in financial transactions also increases the risks associated with such transactions, especially from internet based hackers. This is even though the majority of the users are unaware of the potential of such attacks.

2.3.2 Economic Factors

Price of a technology is an important factor that influences the utilization of the technology. In times of increased competition, a distribution channel must organize business processes efficiently so as to reduce distribution costs. In Mobile Banking, there are three costs: normal costs associated with mobile phone providers' activities, the bank cost and charges and the cellular phone cost. The cost of mobile devices though a one-off cost, makes Mobile Banking as costly as other banking. If the cost of mobile devices is very high, this discourages account holders from acquiring them hence impending the utilization of Mobile Banking services, Chavidi *et al* (2004). With the GPRS, the costs advantage is that the subscriber pays for the volume of the transmitted data and not the time required in the process, Toh (2002) making it the first technology that can not only enable but also promote mobile banking. For instance, in Philippines, domestic and international remittances offer a large market given the large volume transacted and relative low cost of using SMS based mobile phone banking applications as compared to the high cost of current banking and remittance company alternatives, Agabin (2007).

In Germany, findings by Tiwari and Buse (2007), found out that Mobile Payment is preferred primarily for smaller amounts. To further lower the cost of mobile banking the researchers argue that banks can increase the volume of utilization to enjoy economies of scale. The dilemma however is that banks on the other hand demand lower tariffs from the mobile phone network providers in order to increase the volume. As Donner and Tellez (2008), puts it, some forms of impact are already evident: to transfer funds at a distance, especially small amounts of money, mobile banking/m-payments methods are generally less expensive than many of the banking channel alternatives available to poor households. Assuming behaviors of the people do not change and mobile banking users send the same amount of money to the same people with the same frequency, a positive impact would be retention by households of a higher proportion of the money by paying lower fees. In addition to cost-saving, the choice of the word unbanked is evidence of an assumption underpinning much of the policy-makers' and development communities'

interest in the technology. The assumption is that households that currently have no access to financial services will benefit accessing them, Ivatury and Pickens (2006).

Mohamed and Kathy (2008) conclude that price is perceived to be the most important consequence of m commerce utilization compared to convenience, security, privacy and efficiency. As a result, Mobile Banking providers need to pay particular attention to their pricing strategy with the objective to uneven the potential factors that encourage or discourage its utilization. Affordability in mobile banking varies by number, size and type of transactions. Affordable mobile banking often results in indirect impacts like increased incomes, increased family savings rates, and resilience to financial shocks resulting in a change in a family's dynamics on saving and sharing, Reijswoud (2007). People could stay away from their homes longer to make more money to send back home in the form of remittances, Donner and Tellez, (2008). According to Ivatury (2004), using mobile phone technology for micro finance reduces transaction costs considerably, while expanding outreach to rural areas.

Rather than travel to the bank to make their loan payment, clients can text their loan payment directly to the bank; saving travel time and money. This can also benefit the bank if it increases its outreach to rural areas while reducing its costs. However, costs can be driven out of reach of the poor if regulatory requirements like the Anti-Money Laundering rules are not adjusted to permit remote account opening with KYC checks performed by agents and do not take into account the limited formal documentation normally available to low-income clients, Mortimer (2007). A major utilization obstacle is the high charges levied by the Mobile Phone Providers. It would be possible for the regulators to set maximum prices for quota volumes of SMS and other mobile messaging systems which are dedicated to mobile banking systems, Reijswoud &Weir (2007). As these new low-cost (or even zero-cost) mobile banking services emerge, a way for the existing players to keep them out of the game will be to make inter-bank ICT systems unaffordable and/or too complex to be participated in. Regulators can have a role in controlling or eliminating that tendency by setting maximum charges and on insisting on simple but secure interoperability standards, Delgado and Kleijnen (2004).

2.3.3 Social Factors

Conceptualizing electronic money refers to how comfortable people are with electronic money. Donner and Tellez (2008) argue that people coming to banking for the first time

via the mobile handset require a command of abstract concepts about invisible or virtual money. Beliefs, misunderstandings, habits, and concerns must be addressed if people who are used to storing money in cash are asked to store it ―in‖ a handset. It may therefore, be quite a task convincing them that the handset will operate like a wallet thus affecting mobile banking adoption. Hence, adoption will depend on how comfortable a person is with virtual money. Rogers (2013) points out that people react differently to innovation based on their perceived risk of that innovation.

In the social aspect of economic transactions factor there is a long list of social or contextual influences on mobile banking use. Both macro-level cultural factors and micro-level, locally-negotiated norms in families and among peers—particularly about money—are at play. For instance, a person would certainly and very comfortably transfer money to a family member as a gift; however, they would not do so with an acquaintance as a loan. Technically, the actions are the same. Socially, they are miles apart (Donnerand & Tellez, 2008). Attitude towards change is another factor which affects mobile banking adoption. The personal characteristics of mobile banking users determine their adoption decisions (Sulaiman, 2007). For instance, customers or users encouraged by the greater ease and convenience of managing their money are becoming more sophisticated. Also, customers who are savvier are more likely to take control of their money. Hence, as their confidence develops they are more likely to exploit the flexibility of mobile banking. Attitude can also be looked at from the perspective of age of the users. Technology may seem daunting to older people, it is therefore widely assumed that older people are more reluctant or rigid in adopting new ways of doing things including technology. Therefore, this attitude may affect their adoption of mobile banking (Monitise, 2008). Convenience of mobile banking services also plays a major role in the adoption of these services.

2.3.4 Infrastructure

Mobile money transfer is experiencing rapid growth in recent times across the globe. However, upon all the success story of MMT service, there are some potential challenges facing the sector which is affecting the adoption and penetration rate as expected. According to Inter Media (2013:9) research on MMT show that mobile Money has several barriers which inhibit its growth. Poor and unreliable network connectivity is one factor affecting the MMT service (TCRA, 2013). Mostly, due to network connectivity

failures, the service is characterized by a message stating that service is not available please keep trying or try again later and affect the operation of MMVs in the industries.

According to Kenya's Economic Survey of the year 2003, the major Information Systems and mobile technology challenges in the Kenya consist of poor and inadequate information systems, inadequate IT infrastructure, limited skills in ICT, lack of appreciation of ICT, technology weaknesses exhibited by heavy reliance on inappropriate and obsolete technology, lack of skills on modern technology, lack of awareness of the changing technology, poor dissemination mechanisms between and among the various levels of enterprises, and poor technology linkages between the private and public sector institutions.

2.4 Strategies for Mitigating Mobile Banking Risks

As technology continues to evolve with time, it is mandatory for security protocols and procedures to update for users and organizations to continue enjoying its benefits without being concerned about any sort of threats (Gupta, 2015). Several strategies have been adopted by banks to mitigate the threats associated with mobile banking. The current study explores how two factor authentication, encryption, isolation and permission based methods have been used by commercial banks in Kenya to control the prevailing mobile banking risks.

2.4.1 Two factor Authentication

As the use of mobile banking increases, the security and privacy threats of mobile banking through malwares, hacking, unauthorized access and mobile fraud increases. In this context, the traditional login and password authentication is considered insufficient in securing critical applications such as online and mobile banking, while two-factor authentication schemes promise a higher protection level by extending the single authentication factor (Dmitrienko, Liebchen, Rossow, & Sadeghi, 2014). A study by Musaev and Yousoof (2015) to review mobile banking security in Oman shows that two-factor authentication has proven to be a secure method for customer verification as it requires the customers to produce additional authentication together with their unique login identification and password. The additional information may include onetime passcode issued by onetime passcode token or received by mobile short message services, phone call, card reader or a card with random numbers. Dmitrienko et al. (2014) stresses

that two-factor authentication schemes aim at strengthening the security of login password-based authentication by deploying secondary authentication tokens.

However, French (2012) point out that increased security through multiple factor authentication could have negative effect on the mobile banking systems' efficiency since too much information and predefined security questions and answers that needed to be remembered by customers to verify their entry into system lead to decreased perceived usability (Musaev & Yousoof, 2015). Moreover, the use of multiple factor verification should not be taken as fool proof since memorable codes can still be intercepted and used by third parties for unauthorized access or fraud. Despite this, the use of multiple factor authentication offer higher security than single login schemes. The current study explores how commercial banks in Kenya use two factor level authentication schemes in controlling mobile banking threats.

2.4.2 Encryption

Confidentiality of data transmitted through the internet can be achieved by cryptography. According to Soofi, Khan and Fazal-e-Amin (2014) data cryptography is the shuffling of the content of the data, such as text, image, audio, video to make the data meaningless, unreadable or invisible during transmission or storage. The process of transforming data into cipher text is called encryption while the process of reversing the cipher text back to its original form is called decryption. The process of encrypting the data with a secret key before exchange or transmission provide another level of secure communication between the sender and receiver (Singh & Jauhari, 2012). This conceals the confidentiality of the data and improves on the data security.

Soofi, Khan and Fazal-e-Amin (2014) explain that the key role of encryption is to protect the data from online attackers and hackers. Encryption is particularly recommended since it combines the benefits of hiding the existence of a secret message with the security of encryption. Kaur and Kumari (2014) advise that since database encryption has the potential to secure data at rest by providing data encryption, especially for sensitive data, avoiding the risks such as misuse of the data, in order to achieve a high level of security, the complexity of encryption algorithms should be increased with minimal damage to database efficiency, ensuring performance is not affected.

A study by Nyamtiga, Sam and Laizer (2013) explain how in securing financial transactions over distrusted networks, standard SMS with the assistance of *SIM application Toolkit* can be used to addresses message integrity issues by deriving a *Message Authentication Code* from a message by feeding it through a *Triple DES* (Data Encryption Standard) algorithm which is sent along with the original message. In this case SIM card encryption is used to ensure confidentiality by encrypting the PIN. Manoj (2011) indicates that the use SIM Application Toolkit allows for the service provider or bank to house the consumer's mobile banking menu within the SIM card. This makes *SIM application Toolkit* the most secure method of mobile banking as it allows the bank to load its own encryption keys onto the SIM card with the banks own developed application.

2.4.3 Isolation

According to Hayikader, Hadi and Ibrahim(2016), isolation attempts to limit an applications ability to access the sensitive data or systems on a device. The concept of isolation is such that execution of certain computer software's demand to have isolation protocol such as administrator privileges otherwise they will not execute. The main aim of an isolation system is therefore to preserve system integrity. Liang, Venkatakrishnan and Sekar (2003) states that data confidentiality can be preserved to the extent that the untrusted application can be prevented from making network communications.

Use of banks issued mobile phone handsets and or SIM cards can be employed to extremely strict access of data by other mobile phone handsets or SIM cards. The technology works by designing applications that download only to the prescribed gargets. That is to say, the bank can highly secure and limit access to financial data and transactions through the bank's owned devices that can tightly control and monitor activities (Mahesh & Hooter, 2013). The other form of isolation is in the system. According to Vokorokos, Baláž and Madoš(2015) netweok isolation means controlling and limiting access during communication on the local network and the internet. The isolation system should block internet access and prevent sending out confidential information, especially when the program has access to the host files. Example of system isolation protocol is through the integration of firewall into an operating system that blocks network access.

In this case according to Ahmad, Rosalim, Beng and Fun (2010), firewall controls and blocks what kind of network traffic that can be accessed through the network. These usually include unauthorized communication or any possibility of attack. Firewalls therefore, help block uninvited guest or unauthorized persons from trying to connect or gain access to any file share that a bank organization has set up but the bank's own activities are not blocked and or interrupted. The current study therefore seeks to establish the isolation techniques employed by commercial banks in Kenya to protect against mobile banking risks.

2.4.4 Permission Based Access

Hayikader et al. (2016) define permissions based access control to involve granting a set of permissions to each application and then limiting each application to accessing device data/systems that are within the scope of those permissions and blocking the applications if they attempt to perform actions that exceed these permissions. Putting this into the perspective of mobile phone applications, Felt, Greenwood and Wagner (2011) writes that in order to protect users from the threats associatedwith third-party codes, modern mobile platforms use applicationpermissions to control access to securityand privacyrelevantparts of the systems. The smartphones are programmed such that users can decide whether to allowindividual applications to access sensitive resources.

Such permissions may include time-of-use systems which prompt users to approvepermissions as needed by applications at runtime. The other options include permission systems that give the user all the previlages to ask developers to declare their applications' permission requirements up-front so that userscan grant them during installation(Felt, Greenwood, & Wagner, 2011). These persmissions ensure that the user's consent is sought upfront and that proper traiging and defense is established in good time.

The most common forms of permission based access include dangerous warnings presented to Android and Windows mobile phone users during the installation of almost every extention or new application system. Some of these request not only seek to run in the mobile device but also indicates what data the application will use and how. Some request specify the type of risks associated with downloading and running a particularly application in the mobile device. For example an android application installation may indicate that the application will access the device's location, network communication,

personal information, storage, hardware, systems tool among other things. Incorporation of these permission based access in mobile banking is critical for mobile banking users to assess the risks of participating or carrying out a transaction before engaging in the act. It gives the user room to evaluate the threat before taking action. The current study therefore explores the extent to which permission based access are employed by commercial banks in Kenya to mitigate against the myriad mobile banking threats facing the industry.

2.5 Chapter Summary

The current chapter reviewed literature on the concept of mobile banking threats. The chapter identified the most common threats and their mitigation strategies. The following chapter covers the methodology that will be employed to actualize the study.

CHAPTER THREE

3.0 RESEARCH METHODOLOGY

3.1 Introduction

This chapter presents the study design, target population, data collection procedure, research procedure and data analysis method that was be used to answer the research questions in chapter one of this study.

3.2 Research Design

The current study adopted a descriptive research design to explicitly identify the risks facing mobile banking in Kenya and the strategies adopted by the commercial banks to address the current threats and potential future threats. The design was appropriate for the current study since the study seeks to express the situation exactly the way it is in the industry. The method also aided in proper data analysis, interpretation, comparisons and identification of trends and relationships (Aggarwal, 2008).

Descriptive design was used to ensure the study objectivity as it limits the researcher's opinions and perceptions in conducting the study. Thus, the design was instrumental in collecting quantitative data whose validity and reliability can be mathematically tested. The quantitative data was further used for predictions and drawing of inferences about the study variables (Harwell, 2011).

3.3 Population and Sampling Design

3.3.1 Population

According to Easton and McColl (2012) a population represent a set of items, people or animals who share common characteristics that are to be studied. The current study population was consisting of 41 information technology managers each from the 41commercial banks registered in Kenya as at 30th June 2016 (CBK, 2016).

3.3.2 Sampling Design

Sampling design is the process of selecting a representative sub section of the population to be studied for the findings to be generalized to the entire population (Cooper & Schindler, 2014).

3.3.2.1 Sampling Frame

A sampling frame defines the list of the population elements from which a sample is drawn for data collection and analysis (Cooper & Schindler, 2014). In the current study, the sampling frame was the 41 commercial banks as listed in the Central Bank of Kenya's website (CBK, 2016).

3.3.2.2 Sampling Technique

Since the population is small (41), in this study no sampling was conducted but the entire population was involved in the study. Thus, a census was conducted.

3.3.2.3 Sample Size

According to Cooper and Schindler (2014) a sample size is representative subset the population to be studied and the findings generalized to the entire population. In the current study, no sample was drawn but a census was conducted targeting information technology managers, customer service, and bank tellers of all the 41 commercial banks in Kenya which makes a total sample size of 123 respondents.

3.4 Data Collection Method

The study employed the use of survey questionnaires to collect quantitative data. The use of a questionnaire was appropriate because questionnaires are stable, consistent, and uniform and offers considerable objectivity in collecting standardized data (Sandakos, 2005). The questionnaire had four part. The first section to collect data on the general demographics. The second part sought to identify the mobile banking threats. The third part explored how commercial banks mitigate the prevailing mobile banking threats while the last section sought to evaluate measures put in place by commercial banks to mitigate against future potential mobile banking threats.

The questionnaire had two sets of questions. Five point Likert questions and open ended questions. Use of Likert type of questions would control responses and ensure focus in answering of the questions. However, open ended questions were used to seek for more depth and clarification on the respondents' opinions.

3.5 Research Procedure

Before the actual study, a pilot study was conducted to test the effectiveness of the data tool in collecting the right information sought from the respondents. Particularly the pilot sought to identify whether the respondents understood the questions as intended. The pilot study helped in identifying ambiguous questions and words for review before the actual study. The study used 5 respondents (10%) of the population to participate in the pilot study as recommended by Mugenda and Mugenda (2009) for social research. The participants used for the pilot study was excluded from the final study to eliminate preconceived opinions about the study.

The data collection process adopted a drop and pick strategy. In this strategy hardcopy questionnaires were distributed to the respondents by the help of a research assistant. The respondents were given a window of 5 working days to complete the questionnaires before the respondents could revisit to collect the duly filled questionnaires for analysis.

3.6 Data Analysis Method

After the data collection, the data will first be coded and entered Statistical Package for Social Sciences (SPSS) for quantitative analysis. Descriptive data analysis methods were used to establish meaning from the data. Measures of central tendency, frequencies and variances was used to summarize the findings into concrete information for drawing conclusions. The data was presented by use of graphs and tables for easy of understanding.

3.7 Chapter Summary

The current chapter present the study methodology to be used to actualize the study objectives. The following chapter will present the study findings.

CHAPTER FOUR

4.0 RESULTS AND FINDING

4.1 Introduction

This chapter presents interpretations and findings of the study based on the research questions. The first discusses general information. The second section provides findings from what risks arise for commercial banks in Kenya because of mobile banking. The second section discusses what challenges arise for commercial banks because of mobile banking? and the third section discusses findings based in what strategies do Kenyan banks employ to mitigate mobile banking risks

4.1.1 Response rate

The response rate is used to find out the statistical power of a test and the higher the response rate the higher the statistical power. 41 questionnaires were distributed and 37 were filled and returned. Hence a response rate of 90% was represented as shown in table 4.1 below

Table 4.1: Response rate

Questionnaires	**Number**	**Percentage**
Filled and collected	37	90
Non-Responded	4	10
Total	**41**	**100**

4.2 General Information

This section presents the results on general information of the respondents who participated in this study.

4.2.1 Work Experience

The study sought to determine work experience of the respondent. The findings revealed that 54.1% of the employees have worked in the organization for less than 5 years. 9% of have worked for 6-10 years and 6% for 11-15 years as shown in figure 4.1 below

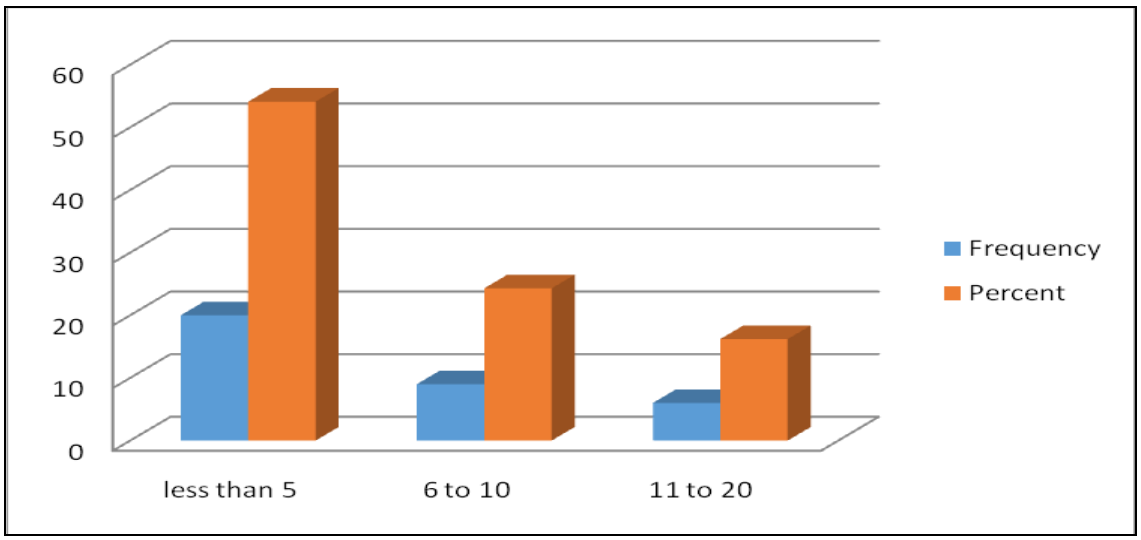

Figure 4.1: Work Experience

4.2.2 Position in the Bank

The study sought to determine Position of respondents in the bank. Findings revealed that middle level had the highest response rate of 64.9%, officer at 16.2%, supervisor and teller at 5.4% and clerk at 2.7% as shown in figure 4.2 below. It was easy to get a hold of employees working at middle level and supervisors as opposed to tellers and clerks.

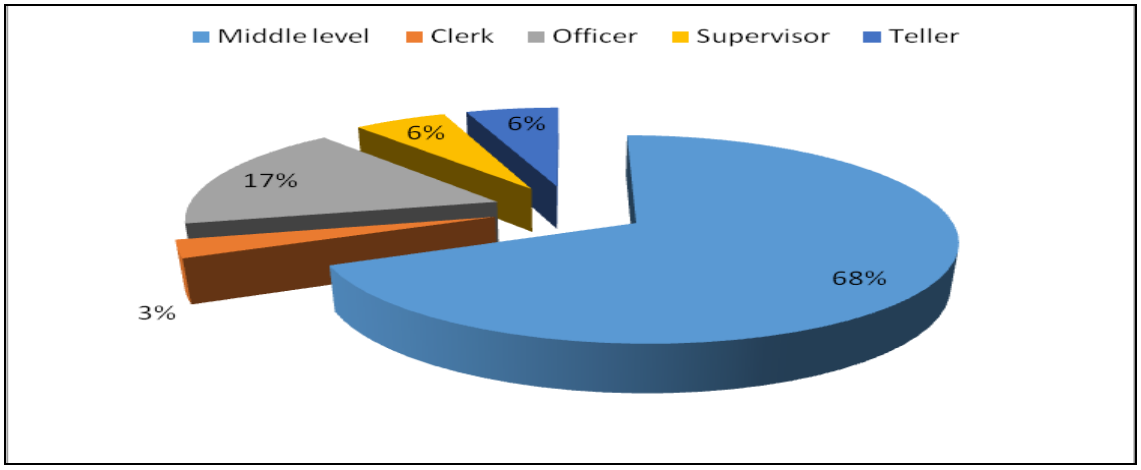

Figure 4.2: Position in the Bank

4.2.3 Education Level

The study sought to determine level of education of the respondents. The study revealed that 49% of the respondents have a bachelor's degree. 37% have a master's degree and 14% have a diploma. As shown in figure 4.3 below. This shows how banks prefer hiring employees who are more educated.

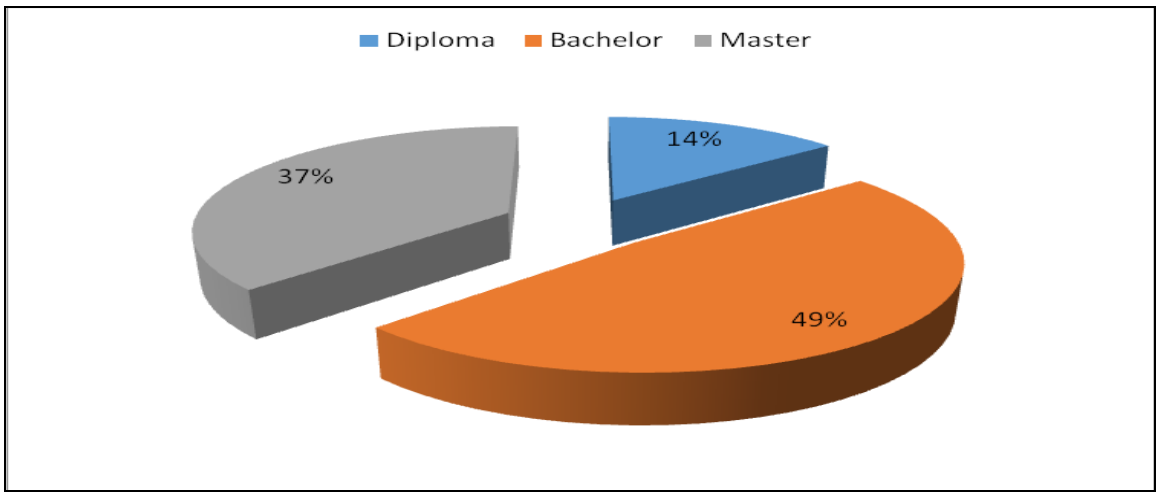

Figure 4.3: Education Level

4.2.4 Work Department

The study sought to determine level of education of the respondents. It was revealed that departments with the highest respondents were customer care and IT which had 8 respondents each representing 22% of the population, while oops had 7 respondents representing 19%, mob banking, teller, and ALT banking had two respondents each accounting for 5.4% whereas credit and manager had 1 respondents each accounting for 3% as shown in table 4.4 below

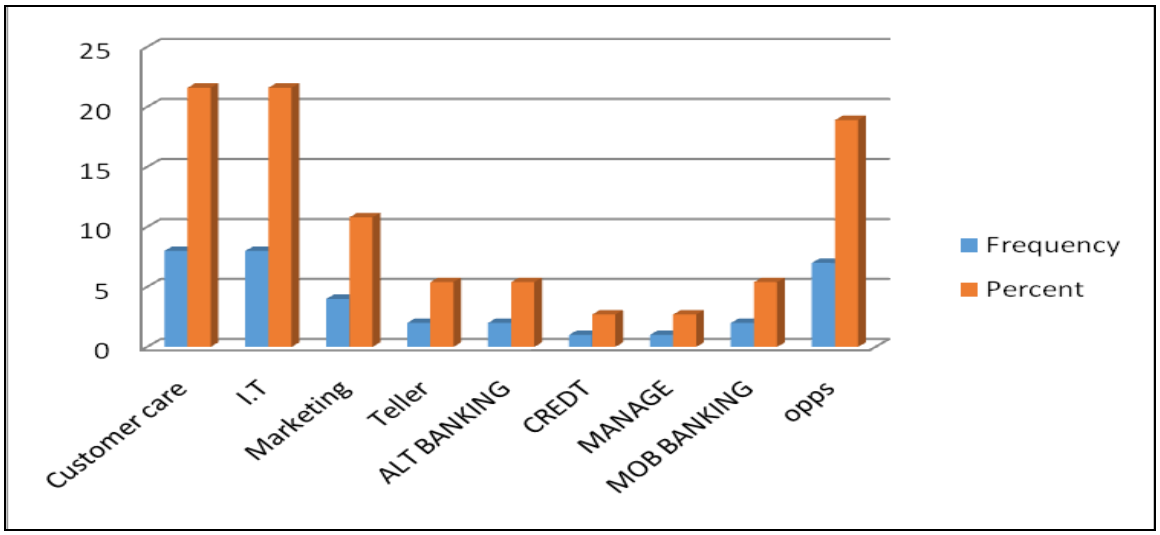

Figure 4.4: Work Department

4.3 Risks arising As A Result of Mobile Banking

The first objective of the study sought to establish risks facing commercial banks in Kenya as a result of mobile banking. The study used a five point Likert scale. Respondents were asked to respond to a set of questions that they were rating with the

least being not at all (1), little extent (2), moderate extent (3), great extent (4), very great extent (5)

4.3.1 Descriptive of Malware

The study sought to determine risks arising as a result of malware and majority of the respondents agreed that there was malware to virus attack on the mobile banking platform (1.78), trojan horses that avoid system security measures on the mobile banking platform (1.73), backdoor attacks that allow secret entry points into the mobile banking programs without normal security check (1.70), botnets which are activated by a certain trigger on a machine to attack and infect other machines (1.68), toolkits which enable root-level access (1.65) and presence of spywares which gather information from our mobile banking platform systems (1.65).As shown in table 4.2 below. Banks have been able to protect themselves from programs from running slow, reduce spam mail and receiving infected mail.

On analysis of the standard deviation virus attack on the mobile banking platform had the highest standard deviation whereas presence of spywares (1.058) which gather information from our mobile banking platform systems (0.919) had the lowest standard deviation. This means that there was a big variation between respondents who agreed, disagreed and neutral.

Table 4.2: Descriptive of Malware

VARIABLE	MEAN	SD
Virus attack on the mobile banking platform	1.78	1.058
Trojan horses that avoid system security measures on the mobile banking platform	1.73	1.045
Botnets which are activated by a certain trigger on a machine to attack and infect other machines	1.68	.973
Presence of spywares which gather information from our mobile banking platform systems	1.65	.919
Toolkits which enable root-level access	1.65	.978
Backdoor attacks that allow secret entry points into the mobile banking programs without normal security check	1.70	1.024

4.3.2 Descriptive of System Hacking

The study sought to determine risks arise from system hacking and a majority of the respondents agreed that there is little extent of system hacking on radical programmers who steal mobile banking PINs and codes (2.22), hackers who secretly read the organization emails (2.00). Moreover it was also agreed that there is no system hacking on programmers who break into the system to transfer customer funds (1.89), radical programmers who break into our web servers to replace information with unwanted content (1.84), hackers who secretly transmit the organization‘s secrets to soft ware’s that will secretly transmit organization secrets to the open Internet (1.73). As shown in table 4.3 below. Banks have been able to develop measures to protect customers information and banks information from being accessed by unauthorized personnel.

On analysis of the standard deviation hackers who secretly transmit the organization‘s secrets to soft ware’s that will secretly transmit organization secrets to the open Internet (1.097) had the highest standard deviation whereas radical programmers who break into our web servers to replace information with unwanted content (0.928) had the lowest standard deviation. This shows that respondents have different views

Table 4.3: Descriptive of System Hacking

VARIABLE	MEAN	SD
Radical programmers who break into our web servers to replace information with unwanted content	1.84	.928
Hackers who secretly read the organization emails	2.00	1.106
Hackers who secretly transmit the organization‘s secrets to soft ware’s that will secretly transmit organization secrets to the open Internet	1.73	1.097
Radical programmers who steal mobile banking PINs and codes	2.22	1.182
Programmers who break into the system to transfer customer funds	1.89	1.063

4.3.3 Descriptive of Unauthorized Access

The study sought to determine unauthorized access in banks and a majority of the respondents agreed that there is little extent of unauthorized access former colleagues using old passwords to gain unauthorized access to our mobile banking system (2.51), unauthorized persons gaining access to mobile banking systems when the users

carelessly leaves their computers it logged on (2.49) and unauthorized access through identity theft were identifying information is acquired through theft in order to impersonate the customer for accessing mobile banking services (2.22). As shown in table 4.4 below. This shows how banks have protected itself from hackers hence protecting company's personal information

On analysis of the standard deviation former colleagues using old passwords to gain unauthorized access to our mobile banking system (1.325) had the highest standard deviation and unauthorized access through identity theft were identifying information is acquired through theft in order to impersonate the customer for accessing mobile banking services (1.228) had the lowest standard deviation. This shows that there was the variation between respondents.

Table 4.4: Descriptive of Unauthorized Access

VARIABLE	MEAN	SD
Unauthorized access through identity theft were identifying information is acquired through theft in order to impersonate the customer for accessing mobile banking services	2.22	1.228
Unauthorized persons gaining access to mobile banking systems when the users carelessly leaves their computers it logged on	2.49	1.239
Former colleagues using old passwords to gain unauthorized access to our mobile banking system	2.51	1.325

4.3.4 Descriptive of Mobile Fraud

The study sought to determine mobile fraud in commercial banks in Kenya and majority of the respondents agreed that there is little extent of mobile fraud on criminal deception by customers for financial gain (2.62), criminal deception by system administrators for financial gain (2.57), criminal deception by agents for financial gain (2.57) and criminal deception by business partners for financial gain (2.19). As shown in table 4.5 below. The organization is able to protect itself from mobile frauds, people phishing for personal information and number being hijacked

On analysis of the standard deviation Criminal deception by agents for financial gain (1.365) had the highest standard deviation whereas criminal deception by system administrators for financial gain (1.214) had the lowest standard deviation hence a small variation between respondents

Table 4.5: Descriptive of Mobile Fraud

VARIABLE	MEAN	SD
Criminal deception by customers for financial gain	2.62	1.233
Criminal deception by system administrators for financial gain	2.57	1.214
Criminal deception by agents for financial gain	2.57	1.365
Criminal deception by business partners for financial gain	2.19	1.244

4.4 Challenges Facing Commercial Banks in Kenya

The second objective of the study sought to establish challenges arising as a result of mobile banking. The study used a five point Likert scale. Respondents were asked to respond to a set of questions that they were rating with the least being not at all (1), little extent (2), moderate extent (3), great extent (4), very great extent (5)

4.4.1 Descriptive of Security

The study sought to determine challenges arising as a result of security and majority of the respondents agreed that there is little extent of security on third party intrusion (2.43) and Loss of privacy (2.41) and that there is little security on hacking (1.95). As shown in table 4.6 below. The results might be due to challenges banks are facing based on security. On analysis of the standard deviation third party intrusion (1.324) had the highest standard deviation and loss of privacy (1.189) had the smallest standard deviation.

Table 4.6: Descriptive of Security

VARIABLE	MEAN	SD
Third party intrusion	2.43	1.324
Hacking	1.95	1.246
Loss of privacy	2.41	1.189

4.4.2 Economic Factors

The study sought to determine challenges arise for commercial banks as a result of mobile banking majority of the respondents agreed there is moderate extent on limited economic factors availability of alternative (competition) (3.03). In addition, there is there is also little extent mobile phone access (2.73) and cost of service (2.61). As shown in table 4.7 below. On analysis of the standard availability of alternative (competition) (1.267) had

the highest standard deviation and mobile phone access (1.189) had the smallest standard deviation.

Table 4.7: Descriptive of Economic Factors

VARIABLE	MEAN	SD
Cost of service	2.61	1.128
Mobile phone access	2.73	1.122
Availability of alternative(competition)	3.03	1.267

4.4.3 Social Factors

The study sought to determine challenges arise for commercial banks as a result of mobile banking majority of the respondents agreed there is limited social factors on customers trust (3.03) whereas limited extent of embracing new technology (2.69) and awareness (2.68). As shown in table 4.8 below. This show that people adopt to use of technology differently hence banks create more awareness and create customer trust and encourage customers to use technology more.

Table 4.8: Descriptive of Social Factors

VARIABLE	MEAN	SD
Embracing new technology	2.69	1.255
Customers trust	3.03	1.185
Awareness	2.68	.884

4.4.4 Infrastructure

The study sought to determine challenges arise for commercial banks as a result of mobile banking majority of the respondents agreed there is little extent infrastructure on network coverage (2.86), reliability service (2.81) and skills of operating (2.20). As shown in table 4.9 below. This might be due to poor and inadequate information systems and inadequate IT infrastructure. On analysis of the standard deviation skills of operating (1.279) had the highest standard deviation, this shows that there was a big variation between respondents.

Table 4.9: Descriptive of Infrastructure

VARIABLE	MEAN	SD
Reliability service	2.81	.786
Network coverage	2.86	.918
Skills of operating	2.20	1.279

4.5 Strategies Kenyan Banks Employ to Mitigate Mobile Banking Risks

The last objective of the study sought to establish strategies Kenyan banks employ to mitigate mobile banking risks. The study used a five point Likert scale. Respondents were asked to respond to a set of questions that they were rating with the least being not at all (1), little extent (2), moderate extent (3), great extent (4), very great extent (5)

4.5.1 Descriptive Of Two Factor Authentication

The study sought to determine strategies employed and respondents agreed that to a greater extent there is use of one time SMS verification codes together with the normal PIN (4.11). Moreover, respondents agreed that there is little extent use of one time phone call verification codes together with the normal PIN (2.74), use of random numbers together with the normal PIN (2.34) and use of card readers codes together with the normal PIN (2.26). As shown in table 4.10 below. The use of two factor authentication is enabling banks to increase customer security. This is because customers are required to provide personal information together with their unique log in identification and password.

On analysis of the standard deviation use of card reader's codes together with the normal PIN (1.502) had the highest standard deviation and Use of one time SMS verification codes together with the normal PIN (1.255) had the smallest standard deviation. This shows that there was a small variation between respondents

Table 4.10: Descriptive of Two factor authentication

VARIABLE	MEAN	SD
Use of one time SMS verification codes together with the normal PIN	4.11	1.255
Use of one time phone call verification codes together with the normal PIN	2.74	1.268
Use of card readers codes together with the normal PIN	2.26	1.502
Use of random numbers together with the normal PIN	2.34	1.259

4.5.2 Descriptive of Encryption

The study sought to determine the level of use of encryption by commercial banks majority of the respondents agreed that a great extent there is use of data encryption to achieve a high level of security (4.34), use of data encryption to avoid misuse of data (4.09). In addition, respondents agreed that there is limited use of data encryption sensitive data (3.83) and use of SIM application Toolkit for PIN encryption (3.58). As shown in table 4.11 below. Banks are able to provide high level of security and encrypt sensitive data hence avoid misuse of data.

On analysis of the standard deviation use of card reader's codes together with the normal PIN (1.502) had the highest standard deviation and use of one time SMS verification codes together with the normal PIN (1.255) had the smallest standard deviation. This shows that there was a big variation between respondents

Table 4.11: Descriptive of Encryption

VARIABLE	MEAN	SD
Use of SIM application Toolkit for PIN encryption	3.58	1.393
Use of data encryption sensitive data	3.83	1.071
Use of data encryption to avoid misuse of data	4.09	.981
Use of data encryption to achieve a high level of security	4.34	.998

4.5.3 Descriptive of Isolation

The study sought to determine the level of use of isolation by commercial banks majority of the respondents agreed that there is limited use of firewall to block network access (3.49). Additionally, respondents agreed that to a little extent there is use of bank's issued SIM CARDS to enhance security (2.60) and use of bank's issued mobile phone handsets to enhance security (2.17). As shown in table 4.12 below.

a great extent there is use of data encryption to achieve a high level of security (4.34), use of data encryption to avoid misuse of data (4.09). In addition, respondents agreed that there is limited use of data encryption sensitive data (3.83) and use of SIM application Toolkit for PIN encryption (3.58). As shown in table 4.12 below. This shows that banks are able to block internet access and prevent sending out confidential information and restrict access of data by unauthorized users.

On analysis of the standard deviation use of bank's issued SIM CARDS to enhance security (1.612) had the highest standard deviation whereas use of banks issued mobile phone handsets to enhance security (1.272) had the smallest standard deviation. This shows that there was a small variation between respondents

Table 4.12: Descriptive of Isolation

VARIABLE	MEAN	SD
Use of bank's issued mobile phone handsets to enhance security	2.17	1.272
Use of bank's issued SIM CARDS to enhance security	2.60	1.612
Use of firewall to block network access	3.49	1.502

4.5.4 Descriptive of Permission Based Access

The study sought to determine challenges arise for commercial banks as a result of mobile banking majority of the respondents noted that to a moderate extent there is limited Use of time-of-use systems which prompt users to approve permissions as needed by applications at runtime (3.41) and adoption of systems that give the user all the previlages to ask developers to declare their applications' permission requirements up-front so that userscan grant them during installation (3.29). In addition, respondents also agreed that there is little extent to Use of systems that warn users that the application will access the device's location, network communication, personal information, storage, hardware, systems tool among other things (2.83) and use of dangerous warnings presented during the installation of extention or new application system (2.55). As shown in table 4.13 below. This shows that banks are able to provide high security by controlling users' access, reduced administrative and IT costs and low maintenance costs and increased efficiency

On analysis of the standard deviation use of bank's issued SIM CARDS to enhance security (1.612) had the highest standard deviation whereas use of bank's issued mobile phone handsets to enhance security (1.272) had the smallest standard deviation. This shows that there was a small variation between respondents

Table 4.13: Descriptive of Permission Based Access

VARIABLE	MEAN	SD
Use of time-of-use systems which prompt users to approvepermissions as needed by applications at runtime	3.41	1.076
Adoption of systems that give the user all the previlages to ask developers to declare their applications' permission requirements up-front so that userscan grant them during installation	3.29	1.296
Use of dangerous warnings presented during the installation of extention or new application system	2.55	1.394
Use of systems that warn users that the application will access the device's location, network communication, personal information, storage, hardware, systems tool among other things	2.83	1.543

4.6 Correlation

4.6.1 Correlation between Strategies Employed by the Banks against the Risks

A Pearson correlation was done to establish the relationship between strategies employed by the banks against the risks. The study established that there was a positive relationship between Strategy employed and risks witnessed in the bank. However, out of all the relationship between the strategy employed and system hack was significant (p-value<0.05). This implies that the strategy employed have mainly mitigated against system hack.

Table 4.14: Correlation between Strategies Employed By the Banks against the Risks

Variable	Strategy	Malware	System hack	Unauthorized Access	Mobile Fraud
Strategy	1	.179	.392*	.117	.094
		.303	.020	.502	.592
Malware	.179	1	.706**	.544**	.646**
	.303		.000	.000	.000
System hack	.392*	.706**	1	.705**	.707**
	.020	.000		.000	.000
Unauthorized Access	.117	.544**	.705**	1	.882**
	.502	.000	.000		.000
Mobile Fraud	.094	.646**	.707**	.882**	1
	.592	.000	.000	.000	

4.6.2 Correlation between Strategies Employed and the Challenges Witnessed

A Pearson correlation was also done to establish the relationship between strategies employed by the banks and the challenges witnessed. The study established that there was a positive relationship between Strategy employed and challenges witnessed in the bank. However, out of all the variables, the relationship between the strategy employed and Economic factor, social factor and infrastructure was significant (p-value <0.05). This implies that the strategy employed have mainly mitigated against challenges related to economic factor, social factor and infrastructure

Table 4.15: Correlation between Strategies Employed and the Challenges Witnessed

Variable	Strategy	Security	Economic Factor	Social Factor	Infrastructure
Strategy	1	.264	.534**	.408*	.465**
		.125	.001	.015	.005
Security	.264	1	.602**	.279	.515**
	.125		.000	.094	.001
Economic Factor	.534**	.602**	1	.409*	.495**
	.001	.000		.012	.002
Social Factor	.408*	.279	.409*	1	.777**
	.015	.094	.012		.000
Infrastructure	.465**	.515**	.495**	.777**	1
	.005	.001	.002	.000	

4.6.3 Regression between Strategies Employed by the Banks against the Risks

A regression analysis was done between strategies employed by the banks against the Risks and the R square value was 0.251 hence 25.1% of the variations in strategies employed was caused by the variations in risks encountered by the banks as shown in table 4.16

Table 4.16: Model Summary on Strategies Employed by the Banks against the Risks

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.501[a]	.251	.151	.52143	.251	2.515	4	30	.062

a. Predictors: (Constant), mobile fraud, malware, system hack, unauthorized access

An ANOVA analysis was done between strategies employed by the banks against the risks at 95% confidence level, the F critical was 2.515 and the p value was (0.062) therefore showing an insignificant difference in the mean between the variables. Results is illustrated below in table 4.17

Table 4.17: ANOVA on Strategies Employed by the Banks against the Risks

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	2.735	4	.684	2.515	.062[b]
	Residual	8.157	30	.272		
	Total	10.891	34			

a. Dependent Variable: strategy
b. Predictors: (Constant), mobile fraud, malware, system hack, unauthorized access

As per Table 4.18, the equation ($Y= \beta_0+ \beta_1X_1 + \beta_2X_2 + \beta_3X_3$) becomes:

$Y= 2.917-0.144X_1+ 0.541X_2-0.185X_3-0.031X_4$

Where Y is the dependent variable strategy employed

X_1 – Malware

X_2 – System Hack

X_3 –Unauthorized access

X_4 – Mobile Fraud

Table 4.18: Coefficient of Strategies Employed by the Banks against the Risks

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.917	.240		12.176	.000
	Malware	-.144	.169	-.221	-.854	.400
	System Hack	.541	.187	.862	2.887	.007
	Unauthorized Access	-.185	.212	-.360	-.871	.391
	Mobile Fraud	-.031	.216	-.057	-.142	.888

The regression equation illustrated in Table 4.18 above has established that taking all factors into account strategy employed was 2.917. The findings presented also showed that with all other variables held at zero, a unit change in malware would lead to a reduction of strategy employed by -0.144 and a unit change in system hack will also lead to 0.541 change strategy employed. Also a unit change in unauthorized access will also lead to -0.185 change in strategy employed. Moreover, the study also showed that a unit decreases in mobile fraud would result in -0.031 change in strategy. Only the variables system hack was significant ($p<0.05$).

4.6.4 Regression between Strategies Employed by the Banks against the Challenges

A regression analysis was done between strategies employed by the banks against the challenges and the R square value was 0.374 hence 37.4% of the variations in strategies employed was caused by the variations in challenges encountered by the banks as shown in table 4.19

Table 4.19: Model Summary of Strategies Employed against the Challenges

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.611[a]	.374	.290	.47677	.374	4.479	4	30	.006

a. Predictors: (Constant), social factor, security, economic factor, mobile fraud

An ANOVA analysis was done between strategies employed by the banks against the challenges at 95% confidence level, the F critical was 4.479 and the p value was (0.006) therefore showing a significant difference in the mean between the variables. Results is illustrated below in table 4.20

Table 4.20: ANOVA on Strategies Employed by the Banks against the Challenges

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	4.072	4	1.018	4.479	.006[b]
	Residual	6.819	30	.227		
	Total	10.891	34			

a. Dependent Variable: strategy

b. Predictors: (Constant), social factor, security, economic factor, mobile fraud

As per Table 4.21, the equation ($Y= \beta_0+ \beta_1X_1 + \beta_2X_2 + \beta_3X_3$) becomes:

$Y= 2.277+0.122X_1+ 0.246X_2+0.159X_3$

Where Y is the dependent variable strategy employed

X_1 –Security

X_2 – Economic factor

X_3 –Social Factor

Table 4.21: Coefficient of Strategies Employed by the Banks against the Risks

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.277	.312		7.298	.000
	security	.122	.150	.254	.816	.421
	Economic factor	.246	.111	.436	2.219	.034
	social factor	.159	.095	.271	1.677	.104

The regression equation illustrated in Table 4.21 above has established that taking all factors into account strategy employed was 2.277. The findings presented also showed that with all other variables held at zero, a unit change in security would lead to an increase of strategy employed by 0.122 and a unit change in economic factors will also lead to 0.246 change in strategy employed. Also, a unit change in social factor will also lead to 0.159 change in strategy employed. Only the variables economic factor was significant ($p<0.05$).

4.7 Chapter Summary

This chapter has presented results and findings. The first section provided an analysis on general information about the respondents, section two analyzed findings on risks that arise for commercial banks in Kenya as a result of mobile banking, section three provided findings on challenges arise for commercial banks as a result of mobile banking and section four presented findings on strategies Kenyan banks employ to mitigate mobile banking risks. Chapter five discusses the findings, conclusions and recommendations.

CHAPTER FIVE

5.0 DISCUSSION, CONCLUSION AND RECOMMENDATION

5.1 Introduction

This chapter presents the findings established from the data analysis done and summarizes the findings. Subsequently, the findings are also discussed in full of relevant literature to support the results established. Thus, the chapter entails the discussion and conclusions as well as recommendations for further studies.

5.2 Summary of the Findings

The objective of the study was to investigate the risks facing mobile banking among the commercial banks in Kenya. The study seeks to answer three research questions. What risks arise for commercial banks in Kenya as a result of mobile banking? What measures are adopted by commercial banks in Kenya to protect against future mobile banking risks? What strategies do Kenyan banks employ to mitigate mobile banking risks?

The current study adopted a descriptive research design. The design was appropriate for the current study since the study sought to express the situation exactly the way it is in the industry. The current study population will consist of 41 informational technology managers in each of the 41 commercial banks registered in Kenya as at 30th June 2016. However, only 37 response resulting into a 90% response rate.

With regard to the first objective the study sought to determine risks arising as a result of malware and majority of the respondents agreed that there were no reported risks arising from malware virus attack on the mobile banking platform. In addition, majority of the respondents agreed that to some little extent of system hacking on radical programmers who steal mobile banking PINs and codes, hackers who secretly read the organization emails. To determine issues of unauthorized access in banks and a majority of the respondents agreed that there is little extent of unauthorized access by former colleagues and unauthorized persons gaining access to mobile banking systems when the users carelessly leaves their computers it logged on and theft in order to impersonate the customer for accessing mobile banking services. To determine mobile fraud in commercial banks in Kenya and majority of the respondents agreed that there is little extent of mobile fraud on criminal deception by customers, criminal deception by system administrators and agents as well as business partners for financial gain.

The second objective established that challenges arising because of security and to some little extent security on third party intrusion, loss of privacy. Majority of the respondents agreed that to some moderate extent availability of alternative, mobile phone access and cost of service is a challenge exhibited. Respondents also agreed that there is limited social factors on customer's trust, and limited extent of embracing new technology and awareness as well as infrastructure on network coverage, reliability service and skills of operating.

The third objective established that there is a great use of one time SMS verification codes together with the normal PIN. Moreover, respondents agreed that there is little extent use of one time phone call verification codes together with the normal PIN, use of random numbers together with the normal PIN and use of card readers codes together with the normal PIN. To analyze level of encryption by commercial banks majority of the respondents agreed that a great extent there is use of data encryption to achieve a high level of security, use of data encryption to avoid misuse of data. In addition, respondents agreed that there to some extent of data encryption sensitive data and use of SIM application Toolkit for PIN encryption. On use of isolation to some moderate extent banks use firewall to block network access. To moderate extent there is limited Use of time-of-use systems which prompt users to approve permissions as needed by applications at runtime and adoption of systems that give the user all the privileges to ask developers to declare their applications' permission requirements up-front so that user scan grant them during installation.

5.3 Discussion

5.3.1 Risks Arising as A Result of Mobile Banking

With regard to the first objective the study sought to determine risks arising as a result of malware and majority of the respondents agreed that there were no reported risks arising from malware virus attack on the mobile banking platform. This is a good show considering the dangers related to the virus. According to Elhadi, Maarof and Barry (2013) malwares can be differentiated based on whether the software needs or does not need a host program to function; or whether the software produces copies of itself or not. Malwares therefore include computer viruses which try to replicate themselves into other executable codes. There are also trojan horses which are computer programs that are benign and have useful functions however, they have hidden potential malicious functions

that avoid system security measures. Third are worms that self-replicates and disseminates versions of itself across a network (Elhadi *et. al*, 2013).

In addition, the study established that a majority of the respondents agreed that to some little extent the banks have experienced cases of system hacking on radical programmers who steal mobile banking PINs and codes, hackers who secretly read the organization emails. Farsole, Kashikar and Zunzunwala (2010) define hackers as a person who like to tinker with software or electronic systems. That is, a radical programmer who aggressively explores creative solutions to problems. These programmers may use their talents to subvert criminal activities or for malicious and illegal purpose (Falk, 2014). According to Pujitha and Mallu (2013), due to increase in use of mobile banking, chances of mobile hacking for financial benefits have heavily increased with over-the-air mobile data hacking in network path from bank to customer mobile handset including MPIN being the major concern. Pujitha and Mallu (2013) add that this has been made grave by the fact that hackers have the ability to steal bank information using various techniques in duping mobile phone users to believe that they are communicating with a genuine program from the bank while in reality the user is giving away sensitive information to the hackers (Luvanda, Kimani, & Kimwele, 2014).

The study established that there is little extent of unauthorized access by former colleagues and unauthorized persons gaining access to mobile banking systems when the users carelessly leaves their computers it logged on and theft in order to impersonate the customer for accessing mobile banking services. Hayikader, Hadi and Ibrahim (2016) established in their research that unauthorized access includes gaining access to some else's authentication code and using it to access a system or simply gaining access to a computer system when the user carelessly leaves it logged on. This has mainly been attributed to customers' general use of static passwords which can be guessed, forgotten, written down and stolen, or eavesdropped. To determine mobile fraud in commercial banks in Kenya the study established that majority of the respondents agreed that there is little extent of mobile fraud on criminal deception by customers, criminal deception by system administrators and agents as well as business partners for financial gain. According to Webroot (2014), mobile devices present greater opportunity for identity thieves due to less user authentication during data sharing; more focus on user convenience over user security; easier access to data on compromised mobile devices; ease of account and documentaccess via email or cloud storage; unsafe data transmission

over wireless connections and unsecuredpublic Wi-Fi. Hoffmann and Birnbrich (2012) add that mobile banking fraud hurts more than just the financial position of both the banks and their customers. For example, Gates and Jacob (2009) posit that as the banks incur substantial operating costs by refunding customers' monetary losses, bank customers experience considerable time and emotional losses as they have to detect the fraudulent transactions. Mobile banking fraud further erodes customer perception, trust and confidence in the bank products. Thus, mobile banking fraud may damage the bank-customer relationship. It may also increase customer dissatisfaction, which may negatively affect customer loyalty and stimulate switching behavior, thereby hurting the banks' reputation and impeding the attraction of new customers (Hoffmann & Birnbrich, 2012).

5.3.2 Challenges Arising from Mobile Banking Risks

The second objective established that challenges arising because of security and to some little extent security on third party intrusion, loss of privacy. Security is the biggest challenge facing the mobile banking world. The use of wireless technology creates a risk that information was stolen, therefore service providers have to employ the use of highly secure encryption technology to prevent third party data intrusion and losses. Venable Telecommunications (2008) argue that the ubiquitous tools of mobile banking open the door to enormous potential for monetary as well as reputation risk, hence mobile banking service providers have to provide security which is commensurate with the size of the financial institution as well as the complexity of the products and services offered. The mobility of the mobile handset and the nature of wireless communications make it difficult to authenticate a customer, hence this becomes a security concern as well for both the banks and their customers.

Ochuma (2007) laments that the major concern in mobile banking is security and banks and vendors need to address this issue more urgently. He argues that the requirement that a customer needs to transact is personal identification number (PIN)which does not guarantee that the person transacting is the real card holder. Security and privacy issues are the most complicated challenges that need to bead dressed jointly by mobile application developers, wireless network service providers and the banks' IT departments to make users feel more comfortable thereby increasing adoption levels (Venable Telecommunications, 2008).

The findings also revealed that a Majority of the respondents agreed that to some moderate extent availability of alternative, mobile phone access and cost of service is a challenge exhibited. New technology and innovation is believed to present risk for many customers, hence they react differently based on their innate characteristics, the wants and the needs of their companies and the behavior of other buyers. Adoption of innovation therefore depends on relative advantage, compatibility, complexity, triability and observability of the innovation (Rogers, 2013). There are several other factors which have been identified by various researchers as affecting mobile banking adoption and they can be categorized into security, economic, social and infrastructure factors. Donner and Tellez (2008) have given other factors fronted propose that mobile banking usage patterns appear to be largely driven by personal missions and marketing strategies of service providers (Njenga, 2011)

Respondents also agreed that there is limited social factors on customers trust, and limited extent of embracing new technology and awareness as well as infrastructure on network coverage, reliability service and skills of operating. Pegueros (2012) argues that customers' perceptions may not necessarily be irrational when you analyze the security risks of mobile banking. She asserts that the relative immaturity of mobile banking brings many inherent risks in the areas of new technologies, new inexperienced entrants in the field and the complex nature of the supply chain. A majority of these new entrants may be innovative and dynamic but have minimal experience or attention to the area of security. A study conducted by Luvanda *et al* (2014) on Kenyan mobile phone users determined that the majority were more interested with the ease at which they could use their phones to perform financial transactions rather than with the related security issues, in total disregard of the evident manifestation of the latter.

5.3.3 Strategies Employed to Mitigate Mobile Banking Risks

The third objective established that there is a great use of one time SMS verification codes together with the normal PIN. Moreover, respondents agreed that there is little extent use of one time phone call verification codes together with the normal PIN, use of random numbers together with the normal PIN and use of card readers codes together with the normal PIN. As the use of mobile banking increases, the security and privacy threats of mobile banking through malwares, hacking, unauthorized access and mobile fraud increases. In this context, the traditional login and password authentication is considered insufficient in securing critical applications such as online and mobile

banking, while two-factor authentication schemes promise a higher protection level by extending the single authentication factor (Dmitrienko, Liebchen, Rossow, & Sadeghi, 2014).

A study by Musaev and Yousoof (2015) to review mobile banking security in Oman shows that two-factor authentication has proven to be a secure method for customer verification as it requires the customers to produce additional authentication together with their unique login identification and password. The additional information may include onetime passcode issued by onetime passcode token or received by mobile short message services, phone call, card reader or a card with random numbers. Dmitrienko et al. (2014) stresses that two-factor authentication schemes aim at strengthening the security of login password-based authentication by deploying secondary authentication tokens.

To analyse level of encryption by commercial banks majority of the respondents agreed that a great extent there is use of data encryption to achieve a high level of security, use of data encryption to avoid misuse of data. According to Soofi, Khan and Fazal-e-Amin (2014) data cryptography is the shuffling of the content of the data, such as text, image, audio, video to make the data meaningless, unreadable or invisible during transmission or storage. The process of transforming data into cipher text is called encryption while the process of reversing the cipher text back to its original form is called decryption. The process of encrypting the data with a secret key before exchange or transmission provide another level of secure communication between the sender and receiver (Singh & Jauhari, 2012). This conceals the confidentiality of the data and improves on the data security.

In addition, respondents agreed that there to some extent of data encryption sensitive data and use of SIM application Toolkit for PIN encryption. On use of isolation to some moderate extent banks use firewall to block network access. Soofi, Khan and Fazal-e-Amin (2014) explain that the main role of encryption is to protect the data from online attackers and hackers. Encryption is particularly recommended since it combines the benefits of hiding the existence of a secret message with the security of encryption. Kaur and Kumari (2014)

advise that since database encryption has the potential to secure data at rest by providing data encryption, especially for sensitive data, avoiding the risks such as misuse of the data, in order to achieve a high level of security, the complexity of encryption algorithms

should be increased with minimal damage to database efficiency, ensuring performance is not affected.

To moderate extent there is limited Use of time-of-use systems which prompt users to approve permissions as needed by applications at runtime and adoption of systems that give the user all the privileges to ask developers to declare their applications' permission requirements up-front so that user scan grant them during installation.

5.4 Conclusion

5.4.1 Risks Arising as A Result of Mobile Banking

The commercial banks have maintained their technology thus ensuring risks related to malware are continuously avoided. There are however risks in regard to system hacking by radical programmers who steal mobile banking PINs and codes, as well as secretly read the organization emails. The institutions also have internal factors such as unauthorized access in banks by former colleagues and unauthorized persons gaining access to mobile banking systems from carelessly users. Apart from the internal factors the institutions also face issues of mobile fraud on criminal deception by customers, system administrators and agents as well as business partners for financial gain.

5.4.2 Challenges Arising from Mobile Banking Risks

The major challenge exhibited include security on third party intrusion, loss of privacy. In addition, the continuous competition in the sector has also contributed to availability of alternative services, mobile phone access and related cost of service. Other issues include limited social factors on customer's trust, and limited extent of embracing new technology, loss of awareness and limited network coverage.

5.4.3 Strategies Employed to Mitigate Mobile Banking Risks

There is a continued use of one time SMS verification codes together with the normal PIN. Moreover, respondents also enjoy one time phone call verification codes together with the normal PIN, use of random numbers together with the normal PIN and use of card readers codes together with the normal PIN. The banks also use data encryption to achieve a high level of security and use of data encryption also help avoid misuse of data.

5.5 Recommendation

5.5.1 Recommendation for Improvement

5.5.1.1 Risks Arising from Mobile Banking

The commercial banks need to maintain their technology to ensure the related malware risks are continuously avoided. There also a need to beef up the set up ensure cases of system hacking by radical programmers. There is also a need to set up heavy in regard to unauthorized access and mobile fraud.

5.5.1.2 Challenges Arising from Mobile Banking Risks

The commercial banks need to analyze security and set up stringent measures to curb cases of third party intrusion, and loss of privacy. In addition, there is a need to inform the customers of the benefits associated with use of mobile banking service.

5.5.1.3 Strategies Employed to Mitigate Mobile Banking Risks

Banks need to enhance their use of one time SMS verification codes together with the normal PIN. The firms also need to continuously adopt PIN related features and use of data encryption to achieve a high level of security and avoid misuse of data.

5.5.2 Recommendation for Further Studies

The objective of the study was to investigate the risks facing mobile banking among the commercial banks in Kenya. There is a need to undertake further studies to establish the effects of the risks established on the profitability of commercial banks in Kenya.

REFERENCES

Abaenewe, Z. C., Ogbulu, O. M., & Ndugbu, M. O. (2013). Electronic banking and bank performance in Nigeria. *West African Journal of Industrial & Academic Research, 6*(1), 171-187.

Aggarwal, Y. P. (2008). *The Science of Educational Research. A Source Book.* Kurukshetra: Nirmal Book Agency.

Ahmad, M. K., Rosalim, R. V., Beng, L. Y., & Fun, T. S. (2010). Security issues on banking systems. *International Journal of Computer Science and Information Technologies, 1*(4), 168-272.

AlSoufi, A., & Ali, H. (2014). Customers'perception of M-banking adoption in Kingdom of Bahrain: An empirical assessement of the extended TAM model. *International Journal of Managing Information Technology, 6*(1), 1-13.

Azzini, A., Ceravolo, P., Damiani, E., & Zavatarelli, F. (2015). Knowledge driven behavioural analysis in process intelligence. *ATAED*, 97-111.

CAK. (2015). *First Quarter Sector Statistics Report for the Financial Year 2015/2016 (July-September 2015).* Nairobi: Communications Authority of Kenya (CA).

CBK. (2016). *Mobile Payments*. Retrieved 10 19, 2016, from Central Bank of Kenya: https://www.centralbank.go.ke/national-payments-system/mobile-payments/

Central Bank of Kenya. (2016). *Bank Supervision*. Retrieved 10 25, 2016, from Central Bank of Kenya: https://www.centralbank.go.ke/bank-supervision/

Cheng, S., Lee, S.-J., & Lee, K.-R. (2014). User resistance of mobile banking in China: cocus on perceived risk. *International Journal of Security and Its Applications, 8*(2), 167-172.

Cooper, D., & Schindler, P. (2014). *Business Research Methods* (14th ed.). New York, NY: Irwin/ McGraw-Hill.

Denison, D. R., & Neale, W. S. (1999). *Denison Organizational Culture: Facilitator Guide.* Washington DC: Denison Consulting.

Dmitrienko, A., Liebchen, C., Rossow, C., & Sadeghi, A.-R. (2014). Security analysis of mobile two-factor authentication schemes. *Intel® Technology Journal, 18*(24), 138-161.

Easton, V., & McColl, J. (2012). Confidence intervals' in Statistics Glossary. Retrieved 11 20, 2016, from http://www.stats.gla.ac.uk/steps/glossary/confidence_intervals.html

Elhadi, A. A., Maarof, M. A., & Barry, B. I. (2013). Improving the detection of malware behaviour using simplified data dependent API call graph. *International Journal of Security and Its Applications, 7*(5), 29-42.

Falk, C. (2014). *Gray hat hacking: Morally black and white. CERIAS Tech Report, 2004-20.* Lafayette, IN: Center for Education and Research in Information Assurance and Security, Purdue University.

Farsole, A. A., Kashikar, A. G., & Zunzunwala, A. (2010). Ethical hacking. *International Journal of Computer Applications, 1*(10), 14-20.

Felt, A. P., Greenwood, K., & Wagner, D. (2011). The effectiveness of application permissions. *WebApps'11 Proceedings of the 2nd USENIX conference on Web application development-Portland, OR — June 15 - 16, 2011* (pp. 7-7). Berkeley, CA: USENIX Association.

French, A. (2012). A case study on E-Banking security – When security becomes too sophisticated for the user to access their information. *Journal of Internet Banking and Commerce, 17*(2), 1-14.

FSD Kenya. (2016). *SME Banking in Kenya.* Nairobi: FSD Kenya.

FSEC Global. (2016). *Infographic: Investigating the State of Malware*. Retrieved from FSEC Global: http://www.ifsecglobal.com/infographic-investigating-the-state-of-malware/

Gandotra, E., Bansal, D., & Sofat, S. (2014). Malware analysis and classification: a survey. *Journal of Information Security, 5*, 56-64.

Gates, T., & Jacob, K. (2009). Payments fraud: perception versus reality – a conference summary. *Economic Perspectives, 33*(1), 7-15.

GSMA. (2016). *The Mobile Economy: Africa 2016.* GSMA.

Gupta, U. (2015). *Application of Multi factor authentication in Internet of Things domain.* Pittsburgh, PE: Carnegie Mellon University.

Harwell, M. R. (2011). Research design: Qualitative, quantitative, and mixed methods. In C. Conrad, & R. C. Serlin (Eds.), *The Sage handbook for research in education: Pursuing ideas as the keystone of exemplary inquiry* (2nd ed.). Thousand Oark.

Hayikader, S., Hadi, F. N., & Ibrahim, J. (2016). Issues and security measures of mobile banking Apps. *International Journal of Scientific and Research Publications, 6*(1), 36-41.

He, W., Tian, X., & Shen, J. (2015). Examining Security Risks of Mobile Banking Applications through Blog Mining. *Research Gate*, 1-6.

Heggestuen, J. (2014). *The Future of Mobile and Online Banking: 2014.* Retrieved 10 25, 2016, from http://www.businessinsider.com/the-future-of-mobile-and-online-banking-2014-slide-deck-2014-10?op=1

Hoffmann, A. O., & Birnbrich, C. (2012). The impact of fraud prevention on bank-customer relationships: an empirical investigation in retail banking. *International Journal of Bank Marketing, 30*(5), 390-407.

Information and Privacy Commissioner (IPC). (2014). *Identity Theft. A Crime of Opportunity.* Ontario, Canada: IPC.

ISACA. (2011). Mobile Payments: Risk, Security and Assurance Issues. *An ISACA Emerging Technology White Paper November 2011.* ISACA.

Islam, S. (2014). Systematic literature review: Security challenges of mobile banking and payments system. *International Journal of Science and Technology, 6*(7), 107-116.

Islam, S. (2014). Systematic Literature Review: Security Challenges of Mobile Banking and Payments System. *International Journal of u- and e- Service, Science and Technology, 7*(6), 107-116.

Joubert, J., & Belle, J.-P. V. (2013). The role of trust and risk in mobile commerce adoption within South Africa. *International Journal of Business, Humanities and Technology, 3*(2), 27-38.

Ju, Y. W., & Lee, B. H. (2013). The implementation of secure mobile biometric system. *International Journal of Bio-Science and Bio-Technology, 5*(4), 53-60.

Kaur, A., & Kumari, S. (2014). Secure database encryption in web applications. *International Journal of Advanced Research in Computer and Communication Engineering, 3*(7), 7606-7608.

Kombe, S. K., & Wafula, M. K. (2015). Effects of internet banking on the financial performance of commercial banks in Kenya a case of Kenya Commercial Bank. *International Journal of Scientific and Research Publications, 5*(5), 1-10.

KPMG. (2016). *Mobile Banking 2015 2 July 2015.* KPMG.

Liang, Z., Venkatakrishnan, V. N., & Sekar, R. (2003). Isolated Program Execution: An Application Transparent Approach for Executing Untrusted Programs. *ACSAC '03 Proceedings of the 19th Annual Computer Security Applications Conference* (p. 182). Washington, DC, : IEEE Computer Society.

Luvanda, A., Kimani, S., & Kimwele, M. (2014). Lack of awareness by end users on security issues affecting mobile banking: a case study of Kenyan mobile phone end users. *Journal of Information Engineering and Application, 4*(5), 19-28.

Mahad, M., Mohtar, S., & Othman, A. A. (2016). Examining the influences of risks towards adoption of mobile baning in Malaysia: an extended decomposed theory of planned behaviour. *Labuan e-Journal of Muamalat and Society, 10*, 1-15.

Mahad, M., Mohtar, S., Yusoff, R. Z., & Othman, A. A. (2015). Factor affecting mobile adoption companies in Malaysia. *International Journal of Economics and Financial Issues, 5*, 84-91.

Mahesh, S., & Hooter, A. (2013). Managing and securing business networks in the smartphone era. *Management Faculty Publications, 5*.

Malhotra, P., & Singh, B. (2009). The impact of internet banking on bank performance and risk: The Indian experience. *Eurasian Journal of Business and Economics, 2*(4), 43-62.

Manoj, V. B. (2011). SMS based secure mobile banking. *International Journal of Engineering and Technology, 3*(6), 472-479.

Manyika, J., Chui, .. M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Byers, A. H. (2011). *Big data: The next frontier for innovation, competition, and productivity.* McKinsey Global Institute. Retrieved 11 20, 2016, from http://www.mckinsey.com/Insights /MGI/Research/Technology_and_Innovation/Big_data_The_next_frontier_for_ innovation

Masamila, B. (2014). State of mobile banking in Tanzania and Security Issues. *International Journal of Network Security & Its Applications, 4*, 53-64.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work, and Think.* Boston: Houghton Mifflin Harcourt.

McAfee Labs. (2016). *McAfee Labs Report Reveals New Mobile App Collusion Threats*. Retrieved from Intel Newsroom: https://newsroom.intel.com/news-releases/mcafee-labs-report-reveals-new-mobile-app-collusion-threats/

MEF. (2016). *Global Mobile Money Report 2015*. Retrieved 10 24, 2016, from Mibile Ecosystem Forum: http://mobileecosystemforum.com/initiatives/global-mobile-money-initiative/global-mobile-money-report-2015/

Mellers, B., Stone, E., Atanasov, P., Rohrbaugh, N., Metz, S. E., Ungar, L., . . . Tetlock, P. (2015). The psychology of intelligence analysis: drivers of prediction accuracy in World politics. *Journal of Experimental Psychology: Applied, 21*(1), 1-14.

Mo, Z., & Li, Y. (2015). Research of big data based on the views of technology and application. *American Journal of Industrial and Business Management, 5*, 192-197.

Morgan, L. (2015). *Hacking vs unauthorised access – what's the difference?* Retrieved 11 15, 2016, from IT Governance Blog: http://www.itgovernance.co.uk/blog/hacking-vs-unauthorised-access-whats-the-difference/

Mudiri, J. L. (2012). *Fraud in Mobile Financial Services.* Luknow, India: MicroSave.

Mugenda, A., & Mugenda, O. (2009). *Research Methods: Quantitative and Qualitative Approaches.* Nairobi, KE: ACTS.

Muiruri, J. K., & Ngari, J. M. (2014). Effects of financial innovations on the financial performance of commercial banks in Kenya. *International Journal of Humanities and Social Science, 4*(7), 51-57.

Musaev, E., & Yousoof, M. (2015). A review on internet banking security and privacy issues in Oman. *ICIT 2015 The 7th International Conference on Information Technology*, (pp. 365-369). Oman.

Ngango, A., Mbabazize, M., & Shukla, J. (2015). E-banking and performance of commercial banks in Rwanda. *European Journal of Accounting Auditing and Finance Research, 3*(4), 25-57.

Nyamtiga, B. W., Sam, A., & Laizer, L. S. (2013). Enhanced security model for mobile banking systems in Tanzania. *International Journal of Technology Enhencements and Emerging Engeering Research, 1*(4), 4-20.

Okiro, K., & Ndungu, J. (2013). The impact of mobile and internet banking on performance of financial institutions in Kenya . *European Scientific Journal, 9*(13), 146-161.

Opili, E., & Muturi, W. (2016). Factors influencing the use of mobile banking in Kenya, the case of M-Kesho in BUNGOMA County. *International Journal of Management and Commerce Innovations, 3*(2), 149-154.

Phua, C., Lee, V., Smith, K., & Gayler, R. (2005). A comprehensive survey of data mining-based fraud detection research. *Artificial Intelligence Review* , 1–14.

Priya, A. S., & Raj, R. K. (2015). Effect of risk factors in the penetration of mobile banking in India-an empirical study. *Middle-East Journal of Scientific Research, 23*(11), 2633-2638.

Pujitha, S., & Mallu, B. V. (2013). SMS based mobile banking. *International Journal of Engineering Trends and Technology, 4*, 1211-1219.

Purcell, B. (2014). The emergence of "big data" technology and analytics. *Journal of Technology Research*, 1-6.

Rosen, T. v. (2013). *Branchless Bnaking in Kenya. Does Mobile Bnaking and Agent Banking have the Potential to lift the Welfare of Low-Come Individuals* . Lund University.

Sakhare, P. S., & Chirayil, D. Y. (2015). M-banking verification using OTP and biometrics. *International Journal of Technical Research and Applications, 31*, 117-225.

Samhouri, M., Al-Ghandoor, A., Ali, S. A., Hinti, I., & Massad, W. (2009). An intelligent machine condition monitoring system using time-based analysis: neuro-fuzzy versus neural network. *Jordan Journal of Mechanical and Industrial Engineering, 3*(4), 294 - 305.

Sandakos, S. (2005). *Social Research* (3rd ed.). New York, NY: Palgrave Macmillan.

Sharma, A., & Panigrahi, P. K. (2012). A review of financial accounting fraud detection based on data mining techniques. *International Journal of Computer Applications, 39*(1), 0975 – 8887.

Simpson, J. (2002). The impact of the internet in banking: Observations and evidence from developed and emerging markets. *Telematics and Informatics, 19*, 315-330.

Singh, A., & Jauhari, U. (2012). Data security by preprocessing the text with secret hiding. *Advanced Computing: An International Journal, 3*(3), 63-74.

Soofi, A. A., Khan, M., & Fazal-e-Amin. (2014). Encryption techniques for cloud data confidentiality. *International Journal of Grid Distribution Computing, 7*(4), 11-20.

Sujithra, M., & Padmavathi, G. (2013). Biometric system penetration in resources constrained mobile devices. *International Journal on Bioinformatics & Biosciences, 3*(1), 35-43.

Vokorokos, L., Baláž, A., & Madoš, B. (2015). Application security through sandbox virtualization. *Acta Polytechnica Hungarica, 12*(1), 83-101.

Wang, J., Liao, Y., Tsai, T., & Hung, G. (2006). Technology-based financial frauds in Taiwan: issue and approaches. *IEEE Conference on: Systems, Man and Cyberspace Oct (2006)*, (pp. 1120–1124).

Wang, S., & Liu, J. (2011). Biometrics on mobile phone, Recent Application in Biometrics. (J. Yang, Ed.) Retrieved from http://www.intechopen.com/books/recentapplication-in-biometrics/biometrics-on-mobile-phone

Webroot. (2014). *The Risks & Rewards of Mobile Banking Apps.* Broomfield, Colorado: Webroot.

APPENDICES

Appendix A: Cover Letter

P.O. Box 14634, 00800
NAIROBI
Date:……

Dear Respondent,

RESEARCH QUESTIONNAIRE

I am a graduate student at United States International University-Africa pursuing degree of Master of Business Administration (MBA).I am conducting a research on the risks facing mobile banking in Kenya. I am using commercial banks in Kenya as case study.

The findings was significant to the management of financial institutions in Kenya by highlighting risks associated with mobile banking. This information was critical in reevaluating and redesigning the mobile banking systems to achieve a reduction on the risks and enhance organizational performance.

This is an academic research and confidentiality is strictly emphasized, your name will not appear anywhere in the report. Kindly spare 15 minutes to complete the questionnaire attached.

Thank you.

Yours sincerely,

Njau John.

Appendix B: Questionnaire

The purpose of this questionnaire is to identify the mobile banking risks in Kenya. Kindly, respond by either selecting the response among choices given that best represents to your views or by filling the spaces provided.

PART I: GENERAL INFORMATION

1. Name of Bank
   (Optional)……

2. Work Experience?

   Less than 5 years [ ] 6-10 years [ ]

   11-15 years [ ] above 15 years[ ]

3. Position in the bank hierarchy?

   Senior Manager [ ] Middle level Manager[ ]

   Other (Specify)……..

4. Highest Education Level?

   Certificate [ ] Diploma [ ]Higher national Diploma [ ] Bachelors [ ]

   Masters [ ] PhD [ ] Other
Specify……

5. Work Department

   Customer Care [ ] I.T. [ ] Marketing [ ] Teller [ ]

[ ] Other specify ……..

PART II: MOBILE BANKING RISKS

To what extent do you encounter the following risks as a result of mobile banking……..

(1- Not at all, 2-little extent, 3-moderate extent, 4-great extent, 5- very great extent)

	1	**2**	**3**	**4**	**5**
Malware					
Virus attack on the mobile banking platform	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Trojan horses that avoid system security measures on the mobile banking platform	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Backdoor attacks that allow secret entry points into the mobile banking programs without normal security check	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Presence of spywares which gather information from our mobile banking platform systems	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Toolkits which enable root-level access	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Botnets which are activated by a certain trigger on a machine to attack and infect other machines	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
System Hacking					
Radical programmers who break into our web servers to replace information with unwanted content	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Hackers who secretly read the organization emails	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Hackers who secretly transmit the organization‘s secrets tosoft wares that will secretly transmit organization secrets to the open Internet	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Radical programmers who steal mobile banking PINs and codes	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Programmers who break into the system to transfer customer funds	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Unauthorized Access					
Former colleagues using old passwords to gain unauthorized access to our mobile banking system	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Unauthorized persons gaining access to mobile banking systems when the users carelessly leaves their computers it logged on	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Unauthorized access through identity theft were identifyinginformation is acquired through theft in order to impersonate the customer for accessing mobile banking services	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Mobile Fraud					
Criminal deception by customers for financial gain	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Criminal deception by agents for financial gain	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Criminal deception by business partners for financial gain	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Criminal deception by system administrators for financial gain	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**

PART III: CHALLENGES OF MOBILE BANKING

To what extent do you encounter the following challenges as a result of mobile banking……..

(1- Not at all, 2- little extent, 3-Moderate extent, 4-Great extent, 5- Very great extent)

	1	**2**	**3**	**4**	**5**
Security					
Third party intrusion	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Hacking	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Loss of privacy	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Economic factors	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Cost of service					
mobile phone access	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Availability of alternative(competition)	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Social factors	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Embracing new technology	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Customers trust					
awareness	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
infrastructure	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Reliability service	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Network coverage	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Skills of operating					

What other measures have been put in place by your organization to safeguard against mobile banking challenges?

……

……

…

PART IV: STRATEGIES TO MITIGATE PREVAILING MOBILE BANKING THREATS

To what extent does your bank employ the following measures to control the current mobile banking risks…?
(1- Not at all, 2-Little extent, 3-Moderate extent, 4-Great extent, 5- Very great extent)

	1	**2**	**3**	**4**	**5**
Two factor authentication					
Use of one time SMS verification codes together with the normal PIN	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Use of one time phone call verification codes together with the normal PIN	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Use of card readers codes together with the normal PIN	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Use of random numbers together with the normal PIN	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Encryption					
Use of SIM application Toolkitfor PIN encryption	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Use of data encryptionsensitive data	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Use of data encryption to avoid misuse of data	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Use of data encryption to achieve a high level of security	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Isolation					
Use of bank's issued mobile phone handsets to enhance security	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Use of bank's issued SIM CARDS to enhance security	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Use of firewall to block network access	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Permission Based Access					
Use of *time-of-use systems* which prompt users to approvepermissions as needed by applications at runtime	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Adoption of systems that give the user all the previlages to ask developers to declare their applications' permission requirements up-front so that userscan grant them during installation	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Use of dangerous warnings presented during the installation of almost every extention or new application system	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**
Use of systems that warn users of that the application will access the device's location, network communication, personal information, storage, hardware, systems tool among other things	**[ ]**	**[ ]**	**[ ]**	**[ ]**	**[ ]**

What other measures are put in place in your organization to mitigate current mobile banking
risks?.....
.....
.....

THANK YOU FOR TAKING PART IN THE STUDY