

**IMPACT OF CYBERCRIME ON THE FINANCE SECTOR: A CASE OF
BANKS IN NAIROBI COUNTY, KENYA (2008 - 2022).**

IBRAHIMNUR ABDI ADAN

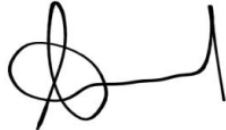
C50/5205/2017

**A RESEARCH PROJECT SUBMITTED TO THE DEPARTMENT OF
POLITICAL SCIENCE & PUBLIC ADMINISTRATION IN PARTIAL
FULFULMENT OF THE REQUIREMENTS FOR THE AWARD OF DEGREE
OF MASTER OF ARTS IN STRATEGIC AND SECURITY STUDIES OF THE
UNIVERSITY OF NAIROBI**

March, 2023

Declaration

This research project is my original work and has not been presented for examination or degree award to any other institution or examination body.



6 April 2023

Signature _____

Date: _____

Ibrahimnur Abdi Adan

C50/5205/2017

This project paper has been submitted for review with your approval as the university supervisor.



6 / 4 / 2023

Signature _____

Date: _____

Prof. Fred Jonyo

Supervisor,

Department of Department of Political Science & Public Administration,

University of Nairobi

Acknowledgement

I wish to acknowledge the Department of Political Science and Public Administration, University of Nairobi for their support and encouragement during my study. Specifically, I am forever indebted to the guidance, patience, timely communication and advice accorded to me by my supervisor Prof. Fred Jonyo. His academic support was also instrumental in shaping this work.

I also wish to acknowledge my employer, the Government of Kenya for granting me the opportunity to further my studies. The material and immaterial support have gone a long way in helping me to achieve this academic feat.

Dedication

To my wife, Abdia and my children, Zakir, Yasra, Umaima and Yahya for their patience, support and for allowing me to take time to complete this research project. May this work inspire you to surpass my humble achievement.

Table of Contents

Declaration.....	i
Acknowledgement	ii
Dedication	iii
List of Figures.....	vii
List of Tables	viii
Acronyms and Abbreviations	ix
Abstract.....	x
CHAPTER ONE	1
BACKGROUND OF THE STUDY	1
1.0 Introduction.....	1
1.1 Background to the Study.....	1
1.2 Problem Statement	3
1.3 Research Questions.....	4
1.4 Research Objectives.....	5
1.4.1 Specific Objectives	5
1.5 Justification of the Study	5
1.5.1 Academic Justification.....	5
1.5.2 Policy Justification.....	5
1.6 Scope and Limitation	6
1.7 Definition of Concepts.....	6
LITERATURE REVIEW AND THEORETICAL FRAMEWORK	8
1.8 Introduction.....	8
1.9 Empirical Literature Review	8
1.10 Theoretical Framework	18
1.10.1 Routine Activity Theory (RAT).....	19
1.11 Research Hypotheses	20
RESEARCH METHODOLOGY	21
1.12 Introduction.....	21
1.13 Study Methodology and Design.....	21

1.14 Study Site	21
1.15 Target Population.....	22
1.16 Data Collection	22
1.17 Sampling Technique	22
1.18 Sample Size.....	23
Table 1.0: Sample size	24
Table 1.1: Sample size	24
1.19 Data Analysis	24
1.20 Research Ethics.....	25
1.21 Chapter Outline.....	25
CHAPTER TWO	26
HISTORICAL PERSPECTIVE.....	26
2.0 Introduction.....	26
2.1 History and Trends of Cyber-crime	26
2.2 Cyber-security Strategies, Policies and Legal Frameworks.....	28
CHAPTER THREE	31
DATA ANALYSIS, PRESENTATION, DISCUSSION.....	31
3.0 Introduction.....	31
3.1 Response Rate.....	31
3.2 Respondent Demographic Information	32
3.2.1 Gender.....	32
3.2.2 Age of Respondent.....	32
3.2.3 Respondent Level of Education	33
3.2.4 Type of Financial Institution.....	33
3.3 Financial Impacts of Cybercrimes on the Banking Sector.....	34
3.4 Impacts of Cybercrimes on Bank data in the Banking Sector.....	40
3.5 Cyber Security Measures put in place by the Banking Sector	43
3.6 Challenges facing cyber security measures utilized by the banking sector	47

CHAPTER FOUR.....	54
SUMMARY, CONCLUSIONS AND RECOMMENDATIONS	54
4.0 Introduction.....	54
4.1 Summary of Findings.....	54
4.1.1 Financial Impacts of Cybercrimes on the Banking Sector.....	54
4.1.2 Impacts of Cybercrimes on Bank data in the Banking Sector	55
4.1.3 Cyber Security Measures put in place by the Banking Sector	55
4.1.4 Challenges facing cyber security measures utilized by the banking sector	56
4.2 Conclusion	58
4.3 Recommendations.....	60
4.3.1 Recommendations for Financial Institutions	60
4.3.2 Recommendations for Regulatory Institutions and Banking Sector Associations.....	61
4.3.3. Recommendation to the Government of Kenya.....	62
4.4 Suggestions for Future Research.....	63
References.....	64
Appendices.....	i
Appendix I: Questionnaire.....	i
Appendix II: Interview Guide	v
Appendix III: Consent Letter	vi
Appendix IV: Introduction Letter	vii
Appendix V: NACOSTI Permit.....	viii
Appendix VI: Cyber Security Companies	ix
Appendix VII: Micro-finance Banks in Nairobi County	x
Appendix VIII: Commercial Banks in Nairobi County	xi

List of Figures

Figure 1: Respondent Gender	32
Figure 2: Financial Institution.....	34
Figure 3: Cyber-crime has a Financial Cost on Financial Institutions.....	36
Figure 4: Countering Cybercrime Activities in the Banking Sector has a High Cost	38
Figure 5: Logic of Cyber-security Investment by Financial Institutions	39
Figure 6: Extent of Effects of Cybercrime on FDI in the Banking Sector	40
Figure 7: Types of Data Losses from Cyber-crimes	42
Figure 8: Relation between Finance and Data losses.....	43
Figure 9: Measures used to Prevent Cyber-crime in the Banking Sector	45
Figure 10: Effectiveness of Current Cyber-security Legal Frameworks in Prosecuting and Convicting Cyber Criminals	48
Figure 11: Effectiveness of Regional Cooperation Mechanisms in the Fight against Cyber-crime in East Africa region	50

List of Tables

Table 1: Respondents Age Bracket.....	33
Table 2: Respondents Level of Education	33
Table 3: Type of Cyber-crimes	35
Table 4: Estimated Annual Financial Losses.....	37
Table 5: Common Types of Data Targeted Cyberattacks.....	41
Table 6: Extent of negative impact from data loss cyber-attacks on Kenya's banking sector	42
Table 7: Extent to which Existing Cyber-security Measures Prevent Cyber-attacks in Kenya's Banking Sector.....	46
Table 8: Extent to which Cyber-criminals By-pass Existing Security Measures in Kenya's Banking Sector.....	47
Table 9: Satisfaction with Regulatory Institutions Ability to Implement Cybercrime Prevention Measures in the Banking Sector	47
Table 10: Extent to which state legal frameworks cover cybercrime related issues in the banking sector	48
Table 11: Effectiveness of Banking Sector Cyber Security Measures for Fighting Cyber-crime	49
Table 12: Chi-Square Tests.....	53

Acronyms and Abbreviations

APT	Advanced Persistent Threats
ATM	Automated Teller Machine
BEC	Business Email Compromise
BFIU	Banking Fraud Investigation Unit
CA	Communication Authority
CBK	Central Bank of Kenya
COVID-19	Coronavirus disease 2019
CRB	Credit Reference Bureaus
DDos	Distributed Denial of Service
DFCU	Development Finance Company of Uganda
FBI	Federal Bureau of Investigation
FRC	Financial Reporting Center
FSOR	Financial Sector for Operational Resilience
GDPR	General Data Protection Regulation
ICT	Information Communication and Technology
IGCI	Global Complex for Innovation
KBA	Kenya Bankers Association
KRA	Kenya Revenue Authority
KYC	Know Your Customer
MFBs	Microfinance banks
MRPs	Money Remittance Providers
NATO	North Atlantic Treaty Organization
NHS	National Health Service
NIST	National Institution of Standards and Technology
OECD	Organisation for Economic Co-operation and Development
OTP	One Time Password
PWC	Price Waterhouse and Coopers
RAT	Routine Activity Theory
SPSS	Statistical Package for Social Sciences
UK	Unites Kingdom
US	United States

Abstract

This study examined the impact of cybercrime on Kenya's banking sector. The expansion of the internet and generalization of its use in all domains of activity, has come with challenges especially internet assisted crime which has attracted a lot of public debate with politicians, policy persons and individuals firms from the private sector proposing and enacting sound policies and laws to deal with cybercrime. These laws have however, proven insufficient, with phishing and other related cybercrimes continuing to occur globally. Kenya has also enacted a battery of legal frameworks but the country has not been spared as the Communications Authority stated that cyber threats in Kenya had gone up by 10% in the first three months of 2019. In Kenya, over 56 million cyber threats were recorded. This was an increase from 37.1 million in 2019. This study therefore assessed the financial impacts of cybercrimes on Kenya's banking sector; assessed the impacts of cybercrimes on bank data in Kenya's banking sector; identified cyber security measures put in place by Kenya's banking sector; and lastly examined the challenges facing cyber security measures utilized by Kenya's banking sector. This study covered the period between 2008 and 2022 and it adopted the Routine Activity Theory. This theory states that the occurrence of a crime is informed by the presence of a motivated offender, suitable target and lack of a capable guardian. This study was a case study which was conducted in Nairobi County. The researcher targeted commercial banks and microfinance banks. Further to this, Banking Fraud and Investigation Department (BFIU), Financial Reporting Center (FRC), Communications Authority and cyber security firms were sampled for inclusion in the sampling frame. Data was collected using questionnaires and key informant guides. The qualitative data was analysed using content analysis while quantitative data was analysed using Statistical Package for Social Sciences (SPSS). From the findings of this study, we conclude that Hacking, Mobile banking breaches, identity theft using email compromise/account take over, SIM-swap and collusion with bank staff are major cyber security threats that banks and MFIs face. Secondly, the study concludes that Cyber-crime has a financial cost on financial institutions but Banks and MFIs do not reveal some of the cyber-crime cases and also the figures presented by financial institutions may not be accurate. The study concluded that Ransomware, Phishing and Business Email Compromise (BEC) are the most common data targeted cyber-crimes; some of the measures used by financial institutions against cyber-attacks include use of advanced softwares; use of online and offline security applications; use of personalized accounts with login key; and use of limited access rights feature. One Time Password and Know Your Customer features are also applied to protect clients. Additionally, conclusions show various measures mentioned have not effectively managed cyber-attacks. This is associated with lack of adequate training of staff and disregard for cyber-security structures. Financial institutions are also dissatisfied with implementation of cyber-crime prevention measures by sector regulatory institutions. In another finding, the legal frameworks do not sufficiently cover cyber-crime related issues. Lastly, a lax environment inhibits implementing of sector cyber-security regulations within the banking sector.

CHAPTER ONE

BACKGROUND OF THE STUDY

1.0 Introduction

This chapter discusses the background of this study. It further addresses the problem statement, research questions, research objectives, justification, scope and also defines the key concepts in the study. Further to this the chapter gives an overview of the literature review and theoretical framework and concludes with the methodology that was applied to gather data for this research project.

1.1 Background to the Study

Cybercrime pose a grave danger to the international financial system. The perpetrators of this crime range from state-sponsored to members of organized criminal groups, internet hackers, terrorists and small-time offenders (Oliveira and Stickings, 2016). Technological advancement has substantially changed the landscape and added more threats in the financial sector operations. Financial service institutions have named cyber security as a top concern as cyber-attacks continue becoming more sophisticated, frequent and harder to detect. Cyber-attacks are defined as deliberate efforts with intent to disrupt or steal or alter or destroy data that is in, or is stored on information technology systems. Cyber attackers use a range of tactics that may include finding flaws in softwares; stealing e-mail account passwords (spear phishing); infecting websites with malicious software (malware); and planting software which can lock out the users of a system (ransomware). These attacks have a huge cost and it has become difficult to estimate the costs of malicious cyber activity (Mester, 2019).

The number of cyber-attacks is on the rise globally and financial services continue to be the main targets. Cyber-attacks are considered as attacks on information and communication technological systems. There is a relatively lower risk of prosecution on one hand, while on the other, a relatively extensive availability of easily usable attack tools and cyber-crime support services. The advances in technology have provided an opportunity for criminals while at the same time provided additional opportunities for financial institutions in their aim of preventing and mitigating risks from cyber-attacks (Adelmann et al., 2020). Bouveret (2018) shows that data on cyber incidents remains scarce because there is a lack of common reporting standards and

secondly, there is a general lack of incentives by companies to report. Direct impacts of cyber-attacks are however, recognized to be immense. Business disruptions stifle business operations; fraud directly impacts finances; while data breaches may affect reputation and contribute to huge operational costs resulting from litigations.

Globally, there are a myriad of cases of cyber-attacks on financial institutions. The Bank of America, JPMorgan Chase, U.S Bank and Citigroup among other banks were in 2012 targeted with intent to frustrate clients and cause financial losses to the banks. The Bank of America was in 2014 targeted with a Distributed Denial of Service (DDos) attack that gave hackers remote control over bank computers and servers. In Europe, hackers stole over \$28.3m from Russian banks. One of the largest banks, HSBC has also been attacked in Europe and clients were unable to access their online banking services. These cases led to financial loss or customer frustration or data stealing (Tariq, 2018).

In Asia, the loss of \$ 101 million to hackers by the Central Bank of Bangladesh in 2016 showed how exploitation of the global financial electronic messaging system can cause huge damages to financial institutions. Such dangerous and extremely harmful events have been caused by the demand for online financial services and exploitation of digital transformation (Maurel and Nelson, 2021). Africa has also had its fair share of cybercrimes. In South Africa cyber-attacks increased to unprecedented levels during the COVID-19 era. Attacks on commercial bank targeted information systems and finances. There were also cases of computers being hacked and/or held hostage by cybercriminals who demanded ransoms. Over seven (7) million clients' personal information got exposed in a single incident but the concerned commercial bank gave a lower profile to the extent of financial damages accrued in this cyber-attack (Chigada and Madzinga, 2021).

In Kenya, recent developments show the banking sector witnessed growth in ICT platforms for providing efficient and wide reaching banking services. The adoption of ICT has enabled banks to deliver services through electronic based mediums that include mobile and internet banking facilities. ICT platforms have also enabled agency banking services where deposits and withdrawals are carried out by a contractor who serves as a third party. This has further deepened in the COVID-19 pandemic era in which digitization and automation of services hit a record

high. The banking sector has a huge capital and reserve base which increased from 501.7 billion to 540.6 billion between 2014 and 2015. There was also a huge growth in ATMs which increased from 2613 to 2718 in the same period. The Banking Fraud and Investigation Department (BFIU) records show there has been increased use of ICT in the banking sector. This has brought tremendous benefits as well as losses. However, their records indicate an increased use of ICT related fraud through use of computers, mobile phones, internet banking. This has been blamed on lack of knowledge on computer-based transactions and ineffective prevention and detection controls (CBK, 2015). As noted by Ayuo (2021) cybercriminals have become the most prolific extortionists in Kenya.

From the above background, this study intended to assess the impact of cyber-crime on the banking sector in Kenya.

1.2 Problem Statement

The internet is a noteworthy technological innovation that has revolutionized individual communication, organizational functioning and the conduct of global commerce in recent history. Privatization of computer networking in the 1990s resulted into expansion of the internet and generalization of its use in all domains of activity. Although the internet is still developing, societies are, to varying extents, already dependent on it. Both the developed and developing world depend on the internet, the former has a more pronounced internet use (Castells, 2002). In the developed world, the challenge of internet assisted crime (cybercrime) has attracted a lot of attention with stakeholders agreeing that sound policies should be enacted to curb cybercrime. Developing countries are also vulnerable to cyber-crime and have passed policies and laws to arrest the challenge (Moitra, 2005). These laws have however, proven insufficient as cyber-attacks continuing to occur. Recent examples include the ransom ware attacks of 2017 that targeted European countries and the US. Other attacks include the 2015 global attacks on banks.

In Kenya since 2008 when digitization and internet adoption was implemented in the banking sector, a battery of legal frameworks has been enacted to address cyber-crime issues. The Kenya Information and Communication Act of 1998; the Computer Misuse and Cyber Crimes Act of 2018; and the Data Protection Act of 2019 are but a few. This has however, not stopped cyber

security threats. Cyber-attacks have become rampant and the country has suffered from botnet attacks, malware, phishing, virus attacks, and disclosure of personal information. Cyber-attacks and threats increased by over 10% in the first three months of 2019. In addition, the last three months of 2020 experienced a 50% increase in cyber-attacks which coincided with remote working systems and e-commerce surge made famous by COVID-19 stringent measures (Communications Authority, 2021).

In 2021, Kenya identified over 56 million cyber threats. This is an increase from the 37.1 million which were detected in 2019. Businesses particularly those in the financial sector, are major targets of cyber-attacks. KNBS and CA show that in 2016, businesses lost 18 billion KES while the Central Bank in 2017 warned local lenders of increased cyber-attacks and ICT enabled fraud (Business Daily, 2021). This shows one of the key sectors that is a victim of cybercrime is the banking sector. There is an increase in ICT related crimes in the banking sector. This trend is only likely to persist considering the global surge in cybercrime activities (CBK, 2015). Further, the transition to Work-From-Home approach due to the COVID-19 pandemic meant that digital methods are adopted by the banking sector. Cloud computing, internet and mobile banking as well as digital customer relationship management have raised security concerns as security breaches are on the rise (CBK, 2020). The Kenya Commercial Bank publicized that it prevented 3624 cyber-attacks and also stopped 663 fraud cases in its banks. One of the cases involved an attempt to defraud the bank of Shs. 2 billion (Business Daily, 2021).

From this background, it is evident that cyber-attacks are an existential threat to the banking sector. This study therefore, assessed the impact of cyber-crime on Kenya's banking sector.

1.3 Research Questions

This study was guided by the following research questions:

- i) What are the financial impacts of cybercrimes on banking sector in Nairobi County?
- ii) What are the impacts of cybercrimes on bank data in the banking sector in Nairobi County?
- iii) What are the cyber security measures put in place by the banking sector in Nairobi County?
- iv) What are the challenges facing cyber security measures utilized by the banking sector in Nairobi County?

1.4 Research Objectives

The main objective of this study was to assess the impacts of cybercrime on Kenya's banking sector.

1.4.1 Specific Objectives

- i) To assess the financial impacts of cybercrimes on the banking sector in Nairobi County.
- ii) To assess the impacts of cybercrimes on bank data in the banking sector in Nairobi County.
- iii) To identify the cyber security measures put in place by the banking sector in Nairobi County.
- iv) To examine the challenges facing cyber security measures utilized by the banking sector in Nairobi County.

1.5 Justification of the Study

1.5.1 Academic Justification

An exploration of existing literature on the effects of cybercrime on the financial sector in Kenya largely produced inconclusive results. In the case of the banking sector, the focus was mainly on the commercial banks. Existing studies were not rigorous and were in-exhaustive in terms of the issues covered especially on data and financial losses. This study was therefore conducted with the intention to fill these literature gaps and further expand literature to cover other finance sector actors such as MFIs which have previously been ignored.

1.5.2 Policy Justification

In terms of policy, this study is vital as it helps to inform policy makers and implementers of laws and legal regulation to counter cybercrime in both the public and private sectors respectively. Furthermore, the study is useful to policy makers as it helps them comprehend the challenges at hand which will in turn help to carve out innovative ways to handle this existential threat.

The use of internet banking has been on an increase in recent years. This increase commensurate the multifaceted nature of cyber-crime that has targeted financial institutions globally. This therefore, makes cyber-crime an interesting phenomenon of investigation. Since 2017, global cyber-attacks (e.g. Ransomware) have targeted mainly the industrialized economies which show

such criminal acts remain an existential threat world over. This signals the need for research to understand, deter or manage the inevitable situation of cyber-attacks on diverse sectors.

1.6 Scope and Limitation

This study covered the period between 2008 and 2022. The study settled on 2008 as the entry point since it marks the start of digitisation and internet adoption in the banking sector in Kenya. This study limited itself to exploring the impact of ICT- related crimes on the banking sector. The banks covered are drawn from three categories; foreign commercial banks (operating in Kenya), domestic commercial banks, and micro-finance institutions.

This study encountered some limitations. First, the sensitive nature of this research predisposed the researcher to hardship in accessing information. Financial institutions withheld information partly due to its sensitivity and reputational risks. This researcher however, assured these financial institutions that the study was an academic exercise. Further, the researcher guaranteed confidentiality and anonymity of the institutions as well as participants while reporting the findings. Further to this, the researcher applied for all necessary clearances and permits before the fieldwork.

1.7 Definition of Concepts

Cyber-crime: Wall (2015) defines cybercrime as a term that signify the occurrence of harmful behavior related to a computer and with no particular reference to law. In this study, cyber-crime means criminal activities that involve a computer or a networked device conducted with intent to cause harm and generate profit for the criminals.

Phishing: according to Liao et al. (2017) this is “the act of sending fake messages to the victim, often in the disguise of bank notifications or emails promising monetary gains and romantic relationships, luring the victim into handing over sensitive information such as account number and password, or install malware on the victim’s system”. In this study phishing means social engineered attacks with intent to steal data of an individual e.g. credit card details, for purposes of defrauding the user.

SPAM: this is mostly spam mail distributed in bulk form to advertise products, services, or investments schemes that are fraudulent. Spam is meant to con or trick customers which results

into financial losses (Jahankhani, Al-Nemrat and Hosseinian-Far, 2014). In this study SPAM means a criminal act where internet users are bombarded with emails that may result in fraudulent activity hence, losses for the users.

Malware: this is software that is introduced into an information system with the aim of causing harm to this or other systems. It is also used to subvert them in order to divert users from using intended system (OECD, 2007). In this study malware consisted of a number of malicious software variants designed to get unauthorized access, cause damage to systems and also data.

Identity theft: Identity theft is the acquisition of adequate information about a victim. This information enables an intruder/attacker to access and utilize funds from a victim's account. The intruder may pay for goods and/or services with this information (Anderson et al., 2013). In this study identity theft meant crimes involving activities intended to obtain personal information of another person which is in turn used to commit a crime mostly fraud.

Hacking: this is the illegal breaking in into a computer system by deliberate means where an attacker passes or circumnavigates security measures in order to steal information in the computer or its network (Liao et al., 2017). In this study hacking means the unauthorized entry into computer systems by cyber attackers in order to destroy information, change or steal information.

Cyber security: This is the “collection of tools; policies; security concepts; security safeguards; guidelines; risk management approaches; actions; training; best practices; assurance and technologies that can be used to protect the cyber environment and organization and user assets” (CA, 2017,). In this study cyber security means deliberate efforts to defend computers, computer networks or systems from malicious attacks.

LITERATURE REVIEW AND THEORETICAL FRAMEWORK

1.8 Introduction

This chapter contains the empirical literature review and theoretical model for the study. Literature reviewed shall be outlined and their main ideas explored in relation to this study. The chapter also outlines a theoretical framework applicable in this study and outlines the hypothesis this study intended to test.

1.9 Empirical Literature Review

Oliveira and Stickings (2016) studied financial institutions and cybercrime. They state that in 2015 cybercrime in the US was ranked as a higher national security threat compared to terrorism and espionage. In Britain, cybercrime has been on an increase with the national agencies (National Crime Agency and Action Fraud) recording an increase in cybercrime. Cybercrime presents a rather complex case as the advantage is that criminals benefit from democratization of access to tools of crime and therefore, there is relatively little effort needed to penetrate the system and commit crime with ease and for large profits. Recent trends in the UK show that marketplace criminals are the most prevalent cyber attackers. This group is more dangerous compared to large scale criminal groups as this new brand of attackers have no economic interests but ideological and political purposes. These authors also point out to the fact that in recent times banks and other financial institutions report incidences of cybercrime more than any other crime. Financial institutions face several types of cybercrime that include cyber dependent crimes such as hacking and DoS attacks. These threats rely on the internet. The other type of cybercrime is the cyber-enabled crimes (robbery, fraud) which are facilitated by technology. This study was conducted in Britain and the U.S and therefore, may not capture the dynamics of cybercrime in Africa and particularly, Kenya. The current study therefore brings out the case of Kenya.

Raghavan and Parthiban (2014) argue that the banking sector was some time back simple and reliable. However, the advent of technology has caused a paradigm shift and banks now offer platforms that have made it even easier through online banking. This has not been smooth thought as technological enhancements have also increased fraud with billions of dollars lost in the process. The study established that the key factors identified which reflect patterns why some financial institutions are targeted more than others is due to their market share, number of

clientele, level of security on authentication system and money transfer policies. This study is based on cases in India. Further to this, it lacks an empirical aspect. This therefore, leaves an opportunity for conducting empirical studies which the current study seeks to undertake.

PWC (2014) surveyed on the threats to the financial services sector and reports that 45% of financial services organizations suffered from economic crimes during the period of the survey. The survey was intended to assess the attitude towards economic crime and also to find out the prevalence of cybercrime in the sector. The findings indicate that the financial value of economic crime, and also the number were on an increase during the survey period. Also the methods are constantly changing and becoming sophisticated. Among the top five economic crimes in the financial sector, cybercrime was second only after asset misappropriation. In the same report, financial sector organizations especially retail banks have the highest propensity to suffer from cybercrime. This report focuses on the top five economies and therefore, lacks a perspective of the developing economies of Sub Sahara Africa. The current study therefore, takes a unique perspective and brings out the data and financial impacts of cyber-crime on Kenya, which is a developing economy.

Camillo (2017) studied management of risks for financial institutions and argues that the scale and ambitions of cyber security continues to escalate. The report states that theft against the financial sector by use of malware and other nefarious means in 2015 increased by 80% and they represented 38% of reported cases. The report also indicates that financial services as an industry is the most targeted. The Threat Matrix Digital Identity revealed a 40% increase in cybercriminal activity towards financial institutions costing a whopping US\$28 billion. Camillo (2017) further states that cyber intelligence is a key solution and financial institutions must develop and maintain effective information security programs. Financial institutions need to use data encryption tools and secure their networks. They should also acquire and install sophisticated systems to manage cyber security risks. Risk management as a strategy should involve detailed intelligence and assessment. Cyber intelligence is an effective way in risk management with financial institutions being able to know their enemies and obtaining information on the possible and varied attacks that may affect them. This study focuses on global-wide banks and also financial institutions which may not be the bedrock of finance in developing economies such as

Kenya where other actors such as micro-finance institutions are present. Therefore, the current study explores the case for global banks and other critical actors that make up the banking sector of Kenya.

Pettersson (2012) states that the financial sector has superior levels of protection against malware and unauthorized endpoints but the danger from well-resourced and sophisticated attackers who have researched and learned the craft of penetrating and benefiting financially. Such access costs large corporation to a tune of \$195,000 in damages though a lot of other losses go unreported. Cyber-attacks have the potential to cause global economic effects as the target is normally the key organizations with potential to affect the global institutions. The report also notes that cyber security is not a one size fits all solution as evolution of technology shows threats and vulnerabilities are also varied from one organization to the other. Security features in the financial sector are high but excesses in rights for access, and also the current standards and policies have not been well organized which creates a risk. Malicious attacks are not only catching up with the security but they now cost more to the financial institutions. It is therefore, critical that financial institutions remain on the lookout to keep up with cyber criminals. They will have to update their security policies, infrastructure and systems while at the same time observe best practices in securing their clientele. This study focuses on banks and therefore, leaves out the microfinance institutions. This therefore, leaves an opportunity for the current study to expand the units of analysis and integrate MFIs.

Staal (2015) argues that financial cybercrime continues to increase as digitization progresses. Organizations continue to adopt and rely on the digital network for operations which also increases the chances of clients also suffering from cyber-attacks. The banking, especially online banking services, have been attacked with the attacks varying from one form to another. Cybercrime has greatly impacted financial institutions with financial losses, data breaches and brand damage. It also has a damaging effect on the image and trust accorded by customers and stakeholders. But financial institutions remain unaware and their personnel are ill-equipped to detect or even identify threats till the crime has been committed. This study is a qualitative study that focuses on the finance sector. This may be limiting as the study lacks quantitative data

which is important in understanding the extent of damage. The current study therefore, collected both qualitative and quantitative data from the banking sector.

Chevers (2019) writes on the impacts of cybercrime on e-banking and argues that cyber-crime is becoming frequent, sophisticated and more dangerous. The adoption of e-banking which offers an efficient way to remotely handle financial transactions depends on technology and is famous for increasing product availability and also reducing transaction cost. However, this has been endangered by cyber criminals who find insecure points and commit illegal acts that endanger businesses and their clients. In the U.S in 2016, the FBI noted there were over one million complaints and a 4.6 million dollars loss due to cybercrime. This has had a negative impact on businesses and the economy in general. This study concentrates on the e-banking in the U.S. This was limited and did not involve other services beyond e-banking. This therefore, left an opportunity for the current study to increase scope and bring out the general impacts of cybercrime on financial institutions.

Tariq (2018) studied the impacts of cyber-attacks on financial institutions and found that even though cyber technology has favored financial institutions through providing online services, data storage, networking and digital money; cyber-crimes have become a disease that endangers such operations. The study shows that cyber-crime has been rapidly growing with severe direct and indirect impacts on financial institutions. Part of the preventive measures being deployed includes tightening of any of the internal security in place, training and cyber security audits. This study was conducted in Pakistan which has a different banking landscape compared to that in Kenya. This gap presented an opportunity for the current study to explore the case for Kenya.

Wasuna (2021) reports on cyber-crime in the East Africa region where cyber gangs have targeted banks in Kenya, Uganda and Rwanda. Two cyber gangs i.e. Forkbombo and Silent Cards have terrorized banks and other institutions in the region for years. Forkbombo was in 2017 charged with involvement in a Kshs 3.9 billion loss by the Kenya Revenue Authority (KRA). In 2019, this cyber gang was involved in a cyber-attack where Development Finance Company of Uganda (DFCU) Bank lost 21.4 million Kshs. In the same year the gang siphoned 244 million Kshs from the same bank without notice. The gang was however, pounced on in November 2019 in Kigali in the process of recruiting internal staff of the Equity Bank Kigali branch to aid in a cyber-

attack. The other cyber gang, Silent Cards is notoriously known for executing one of the biggest single heist in Kenya involving 400 million Kshs siphoned from a Kenyan bank. This study concentrated on the impacts of cybercrime and leaves a gap on the measures put in place in the finance sector. This aspect was therefore covered in the current study which explained the cyber security measures employed by the banking sector in Kenya.

Agrawal (2016) argues that technology has advantages for the banking sector and financial institutions. However, risks have also accompanied these advantages. The risks include operational risks, credit risks and market risks. The banking sector has expanded services in order to provide customers with better services through technology though cybercrime has been an issue in all these improvements. Bank information is susceptible to cyber criminals who cause huge monetary losses to the bank and also the customers. Such attacks are launched on the new e-banking mechanism created by banks and this has had huge financial effects on states economies. The cyber-attacks are prevalent in banks information systems, transactional systems, ATMs, credit card and debit cards, internet banking, and mobile banking. Agrawal states that India is among the top five countries in ransomware, theft and phishing. The cyber-crimes prevalent in the banking sector include hacking, credit card fraud, phishing, spyware, keylogging, viruses, spyware, wateringhole, credit card redirection and malware attacks. This study focused on India which has severe level of cybercrime in the banking sector to Kenya. In addition, this study did not venture into the specific issues. Therefore, the current study focused on financial impacts, data impacts of cyber-crime and security measures within the banking sector.

Kenneth and William (2006) report on the threats of cyber warfare on corporation's commercial expansion. They report that there are several trends showing information warfare has overflowed from the military dimension and flowed right into the private or commercial realm which presents a growing threat to managers of organizations information. The trends show that information warfare has shifted into the civilian context where private institutions have become a major target of cybercrimes which go unreported. Network organizations of today have put in place sophisticated defensive mechanisms for instance firewalls, proxy servers and intrusion detection systems but these security mechanisms remain improperly configured and vulnerable

therefore, leaving space for intruders even the low skilled ones. Further to this, there has been a growing affordability of cyber weapons at the disposal of potential attackers. Also cyber technology has increasingly been used in corporate espionage, organized crime and small businesses. The growing demand for cyber-insurance is also evident to the effects of cybercrime in today's business entities and lastly there is a growing demand for information security professionals. This study is majorly a normative study and lacked an empirical basis. This limits the study findings. The current study therefore addressed this and is based on an empirical investigation.

Symantec White Paper (2015) reports on cyber security for financial services. The report indicates that financial institutions take advantage of the mobile, cloud and other technical trends to meet customer needs. However, cyber criminals capitalize on this technology to launch attacks. Financial services are at crosshairs with cyber attackers due to the amount and sensitivity of information they transact. The financial organizations are fighting multiple fronts as the financial fraud cyber attackers have become organized and sophisticated. The report notes that bigger organizations suffer more as they have more information and higher overall costs. This study is based on secondary sources and therefore, lacks primary data to back up its argument. This gap was exploited by the current study which combined primary and secondary data.

Watkins (2014) studied the effects of cyber security on private sector establishments. He observes that the private sector is in charge of a large section of infrastructure and services and this fact makes cyber-attacks extremely dangerous to society. The author notes that cyber espionage is the greatest threat facing the private sector. He estimates that the cost of cybercrime is over \$385 billion. The United Kingdom (UK) suffers between 18 and 27 billion pounds annually while estimates of the US indicate it's roughly \$100 billion. Reports of 2013 indicate that the US received 54% of the cyber-attacks with Russia and India following closely behind. The attacks were majorly from China, US and Canada respectively. Companies that report cyber-attacks suffer 1%-5% drop in stock value. This recent phenomenon has made companies turn to cyber insurance but breaches in the energy sector have become uninsurable due to high costs. In the private sector, the major target firms include financial services, utility companies and energy firms. Watkins (2014) notes that cyber criminals are making enormous profits at the expense

banks with the most advanced criminals making over \$ 100 million annually. The case is further complicated by the fact that cyber criminals are becoming state affiliated which complicates the political aspects. This paper was based on the experience of the private sector in Europe and U.S. which leaves out state entities and other regions e.g. Africa. The current study therefore, involved government banks as well as government regulatory agencies in the finance sector.

Vijayalakshmi, Priyadarshini and Umamaheswari (2021) Studied how cyber-crime has impacted internet banking in India. Findings show that hacking and identity theft are the most common crimes. The cyber-security measures put in place by the banks are most at times outdated and the process of tracking criminals is time consuming. Lastly, the results indicate that the success rate for resolving cases is just 20 per cent. This study recommends that law enforcement should be updated, fast tracking grievances can restore confidence among the clients, and punishments and penalties on the criminals should be systematically exercised. This study focuses on e-banking in India which has a different banking sector compared to Kenya. Therefore, the study left out other important aspects broader than internet banking. This gap was addressed by the current study.

The Financial Sector for Operational Resilience (FSOR) (2016) studied cyber security in the financial sector in Denmark. It indicates that there is a growing tendency for criminals using IT to target the business sector. The amounts involved in these crimes are large. There is an increase in the use of ransomware where criminal encrypt victims computers and demand for a ransom before decrypting the data. Danish banks have also experienced an increase in phishing and sniffing which have brought massive losses to these financial organizations. The report further alludes to the fact that cyber-attacks on the financial sector firms and systems weakens the confidence of clients to the system. The cyber-attacks compromise the whole system with potential effect on financial institutions and in the long run, it may affect the country's financial stability. Individual financial sector organizations strongly focus on IT security that also includes making the systems resilient to attacks. However, the fact that there is extensive interconnectedness in the financial sector leaves loopholes for exploitation by cyber criminals. This report covered the challenges experienced in Denmark. This may therefore, not be relatable to the experience in a developing country like Kenya where the finance sector is not as advanced as Denmark.

Wall (2007) argues that the internet has impacted criminal behavior. In the argument he states that though nations agree cybercrime have become a major problem, the nation's still don't agree on how to tackle the problem collectively. Further to this the problem goes as far as the small number of prosecutions for cybercrimes. The reliability and partiality of information regarding cybercrime has made its prosecution a challenge to organizations and states alike. This study was conducted in 2007 and has therefore, not covered the range of developments within the banking sector such as mobile banking and other innovations. The current study therefore, covered these developments within the sector and updated the innovations that have taken place since 2007.

Cashel et al., (2004) studied the economic impact of cyber-attacks and argue that the number of cyber-attacks have increased in frequency. These authors warn that there is a possibility that future attacks will be more severe. Further to this, these scholars assert that there is a lack of standard methodologies that measure the cost and the frequency of attacks. There is also reluctance by organizations to publicize their experiences. In addition Cashel et al. (2004) reports that investigations on financial impacts of the cyber-attacks shows that firms are dented between 1 and 5% losses after the attacks. In New York the stock exchange companies recorded between \$50 and \$200 million dollars in losses due to cyber-attacks. They conclude that the macroeconomic costs of cyber-attacks remain speculative. This study is old and focuses on financial impacts of cyber-attacks. This leaves a gap for the current study that expanded its scope to include other issues such as impacts of cyber-crime on bank data. In addition, the current study updated the literature with developments in the sector since 2008.

Broadhurst (2006) studied the developments that have taken place within the global cyber-crime law enforcement. Findings of this study indicate that cyber-crime is traditional crime that is accomplished in a swift manner on a vast number of victims. It is unauthorized and damages systems with the most detriment, having malicious interruptions on computer operations on particularly, e-commerce on a global scale. Cyber-crime is of a cross national nature and this renders many policing methods domestic and national, ineffective. The report also discusses the "digital divide" that exists between nation-states. There exists a Convention on Cyber-crime that stipulates members have to criminalize specific offences in Europe. This gives the states an opportunity to have a uniform law governing cybercrimes. The reality today is that digital

footprints are ephemeral and it is difficult to trace offenders over several countries and jurisdictions that have varied regimes. This study focused on law enforcement in Europe and did not capture the dynamics in Africa and Kenya. The current study therefore, saw this as a gap and therefore, expanded its scope to capture the various crimes that have emerged in recent times.

Randazo et al. (2005) studied illicit cyber activities in the bank and finance sector. They found out that insider attacks on financial organizations required minimal technical skills. A large number of cases recorded showed that attackers were successful through exploitation of inadequate policies, practices and procedures. Further to this they recorded that the interaction among organizational culture, policies, business culture, and technology and insider motivation led to cyber-attacks. The report notes it is crucial to involve other factors other than financial performance in the management of financial organizations. The need to improve security of the systems and networks would go far in preventing cyber-attacks. Another finding was that a profile of possible inside perpetrators showed considerable variance in their technical knowledge. This study is old and did not capture developments since 2005. Therefore, this left room for the current study to update the literature as well as developments in the banking and finance sector in Kenya.

Watkins (2014) delves into some of the legislative measures put in place to reinforce the cyber security and help deal with the offenders. He mentions the Convention on Cybercrime (Budapest Convention) put in place in 2004. This was a leading international treaty addressing issues of internet crime by harmonization different national laws. The Convention states that combating cybercrime can only be approached from a global scale. Further to this it seeks to promote cooperation of different industries and also between states and private industry. It emphasizes on public asset security. The UN states that international law addresses cyberspace. The North Atlantic Treaty Organization (NATO) sought to curb hacking through cyber security harmonization among member states. In 2011, NATO developed both a policy and also an Action Plan. These frameworks were geared towards strengthening defense efforts. Lastly, Interpol has an initiative which seeks to establish a Global Complex for Innovation (IGCI). This is based in Singapore and facilitates cross-border collaboration on matters of cybercrime. This

study concentrates on legislative measures and did not comprehensively touch on the impacts of cyber-crime. The current study therefore filled this gap.

Lockheed Martin Corporation (2015) argues that despite the significant steps in the race to strengthen cyber security, financial institutions are challenged by the speed of technological change, and the complex nature of cyber threats. Many institutions are finding it hard to adopt up to date and cutting-edge technologies into their product and service offerings. The risk management practices are used by financial institutions are driven by industrial compliance. This however, leads to adopting of reactionary tactics for security controls and vulnerabilities. Financial institutions historically had adopted security operations centers for purposes of defending the enterprise and responding to security threats. Current security threats require a predictive approach to security where a security intelligence center is a vital part of the organization. This facility is composed of people, capabilities and technology. The report concludes that financial institutions have the opportunity to grow businesses wise and improve operations while at the same time threats will continue to exist. The institutions ought to have active security approaches with vendor propelled detection mechanism, innovative processes and out of the box solutions.

Mugari (2016) writes on cyber-crime in Zimbabwe and argues that it is prevalent in financial institutions of the country. Some of the threats include hacking, spreading malicious software and identity theft which are common cyber threats. In order to curb this challenge, financial institutions have resulted to training, updating softwares and firewalls. Despite these cyber-crime strategies, banks have a problem with keeping up to date as technology continues to change on a daily basis. This study collected evidence from Zimbabwe only. This limited the study and gave an opportunity for other studies. The current study therefore captured the case for Kenya and further assessed the financial and data impacts which were not explored by Mugari.

According to a PWC (2014) report, about 41% of the respondents working in the financial sector believe that they will experience cybercrime in the near future (24 months). Further to this most of the respondents perceive that there will be an increase in cybercrime and the menace is becoming greater than ever before. Further, PWC notes in the financial sector, less than 40% of the economic crimes recorded are acknowledged as cybercrime. However, financial sector

organizations rarely log and identify the cyber aspect of economic crime they experience and therefore such organizations are left exposed to threats despite having cyber-defense mechanisms. Therefore, this means that the true risk posed by cybercrime to financial institutions remains insufficiently understood. This study takes note of the loopholes in the banking sector as of 2014. The current study however, captures part of the problem since 2014 and therefore, updated the literature as well as recent measures that have been put in place.

The Communications Authority of Kenya (CA) (2017) argues that cyber-crime relates to various internet activities that include and are not limited to online impersonation, ransom ware, mobile money fraud, online illegal access to bank accounts, and social engineering. Cyber-attacks target individuals, private entities and governments. In Kenya cyber-attacks have become rampant with botnet attacks, malware, phishing, virus attacks, disclosure of personal information e.g. PINS and passwords through duping, and hacking of technical infrastructure.

Further, the Communications Authority (CA) (2021) noted that cyber threats in Kenya have increased by over 10% in the first three months of 2019. This was attributed to technological advancement which creates opportunities for cyber-crime. This increase is also visible in the global scene where malware such as ransomware was a common type. This increase to 56 Million cyber threats in 2020 from 37.1 million threats in 2019 indicates cyber security is a pertinent issue in Kenya. Threats were mostly malware (46 million), web applications (7.8 million) and Distributed Denial of Service (DDos) (2.2 million). The country now has frameworks including the Kenya Information and Communication Act of 1998, Constitution of Kenya of 2010, the Computer Misuse and Cyber Crimes Act of 2018 and the Data Protection Act of 2019 which combine to govern the cyber security landscape. This report however, fails to capture the banking sector measures applied to prevent cyber-attacks in the sector. This was therefore studied in an in-depth manner by the current research.

1.10 Theoretical Framework

Theories and models have been put across to explain the adoption of technology by institutions. These institutions adopt technology in their management and operations in order to meet various objectives including their security needs. This study applied the Routine Activity Theory which explains issues around crime.

1.10.1 Routine Activity Theory (RAT)

The Routine Activity Theory holds that for a crime to occur, the presence of a motivated offender, presence of a suitable target and lack of a capable guardian must all be in place. Proponents of this theory including Lawrence Cohen, Ronald Clark and Marcus Felson argue that crime is highly dependent on the populations changing lifestyles and behaviors (Clarke and Felson, 2017).

Cohen and Felson (1979) argue that an offender motivated to commit a crime, is driven by crimes of different natures. A suitable object for the offender is dictated by the value and also access to the object. On the other hand, this is governed by the lack of informal or formal control for protecting the object. The Routine Activity Theory sums up crime as an event which depends on offenders' personality and socialization than the situation of the offender (Cohen and Felson, 2012). Further this theory argues that the three aforementioned elements have to converge in time and space for the crime to take place.

The Routine Activity Theory has been applied in studying phishing, which is one of the main cyber-crimes reported today. The increase in numbers of internet users has increased suitable offenders as people become more technologically knowledgeable. On the other end, more internet users and the increased levels of internet banking among technologically able populations has increased numbers of potential victims. Therefore, offenders and potential targets are in large numbers (Hutchings and Hayes, 2009)

In relation to the current study, the Routine Activity Theory captures cyber-crime in the banking sector. The increasing adoption of technology and the internet by banks and their clients provides a suitable target for cyber criminals who have diverse motivations to commit cyber-attacks. Internet banking has provided criminals with a target area. The nonexistence of capable guardianship may relate to the lack of awareness or insufficiency of cyber security measures implemented by the finance sector and the government in general. This theory has been used by previous scholars to study several types of cyber-crime. It will therefore be important in enriching the current study and also enabling the researcher to test its limits in explaining other cyber-crimes.

1.11 Research Hypotheses

H0 (Null hypothesis): That cyber-crime has a negative effect on Kenya's banking sector.

RESEARCH METHODOLOGY

1.12 Introduction

This section contains the methodology adopted by the researcher for this study. It contains the study design, target population, methods of data collection, sampling technique and methods that were applied in the data analysis process.

1.13 Study Methodology and Design

This study adopted a case study design. Yin (2009) states that a case study is an empirical inquiry that seeks to investigate contemporary phenomenon in real time. In the case study, multiple sources of data may be applied and the inquiry benefits from prior theoretical developments. Therefore, the case study research design helped to investigate the impacts of cybercrime on the financial sector. The case study focused on both Commercial (foreign and domestic) and Microfinance Banks in Nairobi County.

1.14 Study Site

Kenya's banking sector comprises of a regulatory body, the Central Bank of Kenya and 42 Banks. This number comprises of 41 Commercial Banks and 1 Mortgage Finance company. The foreign owned banks have 9 representative offices. There are 14 Microfinance banks (MFBs), 3 credit reference bureaus (CRB), an estimated 17 Money Remittance Providers (MRPs), 8 non-operating bank holding companies and lastly there are 66 foreign exchange bureaus (CBK, 2020). However, this study concentrated on the 41 commercial banks and 14 Microfinance institutions based in Nairobi.

This inquiry was conducted in Nairobi County. This County hosts the country's capital city and has the largest number of banks in the country. The banking sector in Kenya is concentrated in the capital city with bank branches or headquarters located here. The net asset base of the sector was Ksh. 5.4 trillion on December, 2020. It is worth noting that Kenya recorded an increase in bank branches from 1490 to 1502 between 2019 and 2020. In this expansion, Nairobi County was the area with the highest increase in physical quantity of bank branches. The commercial banking sector has 9 large banks (74.55% market share), 9 medium banks (17.21% market share) and 21 small banks (8.24% market share). On the other hand, Microfinance (MFBs) are 14 in number and have a total asset base of Ksh. 74.9 billion (CBK, 2020).

As reported by the CBK (2020), the development of digitization has increased usage of cloud services by the banking sector. Cloud services have however, led to rise of cyber-privacy issues that include data infiltration. Cloud usage related risks have given rise to security of the cloud and security in the cloud. Security preparedness has become a necessary requirement which is solved by cyber programs that mitigate cloud based cyber-attacks.

1.15 Target Population

Nachmias and Nachmias (2007) define population as a well-defined set of units of analysis for a study. In this study, the target population included commercial banks and microfinance banks. Further to this, Banking Fraud and Investigation Department (BFIU), Financial Reporting Center (FRC) and cyber security firms were targeted for inclusion in the study.

1.16 Data Collection

The researcher capitalized on both primary and also secondary data.

Primary data was gathered by use of questionnaires and interviews. The questionnaires were semi-structured questionnaires that were filled by the management and technical departments of financial institutions which included commercial banks (foreign and domestic) and micro finance banks. On the other hand, officers of the Banking Fraud and Investigation Unit (BFIU), Financial Reporting Center (FRC) and cyber security companies were interviewed. In this process, the researcher noted that there was need to also interview the Communications Authority of Kenya (CA).

Secondary data was collected from published material and online platforms. These included books, journal articles, government reports, periodicals, published theses, websites and other secondary sources.

1.17 Sampling Technique

Sampling is defined as the process of identifying a subset of a population which helps the researcher to make generalizations about the whole population. The subset is representative of the characteristics of the population (Taherdoost, 2016). This study selected its sampling frame from commercial banks, micro finance banks, Banking Fraud and Investigation Unit (BFIU), Financial Reporting Center (FRC) and cyber security firms. These institutions were sampled

through a combination of purposive (non-probabilistic) and simple random sampling (probability) for inclusion in the sample frame.

In the case of commercial banks (foreign and domestic) and micro financial banks, simple random sampling was applied in order to select banks that were sampled. According to the CBK (2020) there are 17 foreign owned commercial banks, 22 domestic owned banks and 14 microfinance institutions (See appendix VII & VIII). Simple random sampling was applied to draw a sample from each category.

Secondly, the study purposively sampled cyber security firms, Communications Authority of Kenya (CA), Financial Reporting Center (FRC) and the Banking Fraud and Investigation Unit (BFIU). The BFIU and FRC are government institutions in the country created to address various issues related to financial irregularities. The cyber security firms were selected through purposive sampling where the top three companies were purposively selected from the top ten cyber security companies as listed by the Kenya Magazine 2021 (See appendix VI). Experts and officers from these institutions were interviewed for their opinion and information.

1.18 Sample Size

In order to calculate the sample from the population, this study applied the Yamane formula. This method is used to calculate sample size for finite populations. The given sample size therefore, gives proportionately more information when applied to a small population compared to a larger population.

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

Where N is the population, n is the sample size while e is the precision level which is +/- 5%

Using the Yamane formula, the sample was calculated as shown in the table below.

Table 1.0: Sample size

Institution	Population	Sample	Percentage
Foreign owned banks	17	16	32%
Domestic owned banks	22	21	42%
Microfinance banks	14	13	26%
Total	53	50	100%

(Source: Author, 2021).

From the above sample, the researcher used the Random number generator, which is an online scientific random generating platform used to generate random numbers using a minimum and maximum range. This platform helped the researcher to generate a list of random numbers representing the banks. These banks were the sample in the study.

For the Cyber security firms, CA, FRC and BFIU, the sample below was purposively selected for interviews. In this case, purposive sampling was applied due to the specific mandate and expertise of these institutions.

Table 1.1: Sample size

Institution	Population	Sample	Percentage
Cyber security firms	10	3	50%
BFIU	1	1	16.7%
FRC	1	1	16.7%
CA	1	1	16.7%
Totals	13	6	100%

(Source: Author, 2021).

1.19 Data Analysis

According to Yin (2009) data analysis has several steps. It includes examining, categorizing, tabulation and lastly, testing of evidence that will address the propositions of a study. This study applied content analysis to analyse qualitative data and Statistical Package for Social Sciences (SPSS) to analyze quantitative data. Through content analysis the data was checked for

replicable and systematic patterns. This data was then categorized and meaningful inferences extracted. Correlations were thereafter used to report findings. The quantitative data on the other hand was analysed through SPSS. Statistical analysis was conducted to show correlations in the study variables. The findings were presented through tables and charts.

1.20 Research Ethics

The researcher observed necessary research ethics before, during and after field work. First, the researcher applied for all necessary permits and authorization documents before data collection. This included the National Commission of Science Technology and Innovation (NACOSTI) permit (Appendix V) and the University of Nairobi (UoN) Introduction letter (Appendix IV).

In terms of the ethics around data collection, consent was requested from respondents before data was collected from them (Appendix III). This involved using a consent form which respondents signed. Other ethical practices included maintaining anonymity of the respondents, confidentiality of the information, and proper storage of the data.

1.21 Chapter Outline

Chapter one of this study covered the background to the study. It outlined the problem statement as well as the objectives of the study. Further, it covered the justification, scope and limitations. Chapter two of the study contained the literature review and theoretical framework underpinning the study. A research hypothesis was also suggested in this chapter. Chapter three of the study contained the methodology used to collect and analyse data for the study. It outlines the study design, site, target population, sampling process and data analysis. Chapter four of this study focused on analysis and presentation of findings of data. This data was presented in narrative form, tables, charts and using descriptive statistics. Chapter five of the study concentrated on summarizing the study; and giving conclusions and recommendations that may be adopted by the main actors cited in this study.

CHAPTER TWO

HISTORICAL PERSPECTIVE

2.0 Introduction

This chapter gives a historical background of cyber-crime. Further to this the trends and effects from the global, continental and country case are outlined. The chapter also gives a picture of the cyber-security landscape capturing the legal and policy frameworks from around the world and those that Kenya has put in place.

2.1 History and Trends of Cyber-crime

Cybercrime can be traced to the era before emergence of the internet. However, the emergence of the internet marks an undisputed era when the internet allowed criminals new opportunities. In the 1980s emergence of personal computers and increased internet penetration across the globe led to crimes labeled as software piracy and copyright crimes. Globalization in the 1990s led to fast penetration of the internet and the rise of computer networking presented new challenges as criminals exploited vulnerabilities in this networking system. Also in the 1990s, there was an exponential increase in internet users. There was also the emergence of the graphical interface 'www' (Brenner, 2010).

It was however in the 21st century that crime through the internet picked pace with crimes such as phishing and use of bots emerged. In countries such as the U.S, Japan, Australia and the continent of Europe experienced frequent cyber-crimes. There were also new trends in cyber-crime as new crimes emerged in this decade. The Voice-over-IP (VoIP) that capitalized on communication and cloud computing also emerged during this time. There was an increase in magnitude of attacks and the methods of attack. Automation of attacks also presented huge challenges for detection of cyber-crimes (Steinmetz and Yar, 2019).

Cybercrime remains a complex phenomenon which is complicated by first, the various different types of offences. Financial institutions are affected by cyber-crimes especially phishing and malware. The impacts either financial or other intangibles such as customer trust are impacted by cyber-crime. As of 2011, the United Kingdom estimated losses to be around £2.5 billion (Leukfeldt, Lavorgna and Kleemans, 2016).

In Africa penetration of the internet reached the 10% - 15% level, which is the threshold that allows for significant hacking activities. Emerging economies have become major targets as they are considered 'low hanging fruit'. Losses in South Africa were estimated to be \$157 million, Nigeria was \$649 million and Kenya was \$210 million in 2017. Since 2013 trends show an increasing trajectory which is faster than any other region in the world. Financial institutions in Ghana are targeted by Malware and spam emails. Such cyberattacks across the African continent are attributed to lax cyber-security and vulnerable systems. This perception that cyber-security is a luxury and not a necessity, has further endangered businesses. Financial institutions which are the biggest targets from threats lack proper cyber-security practices. As of 2009, 60% of Kenyan banks had insecure systems. By 2011 only 40% of financial institutions in Kenya, Tanzania and Uganda were prepared to handle cyber-threats (Kshetri, 2019).

In Africa many countries have been affected by cyber-crime. The emergence of internet banking with its many benefits also brought about its downsides. Internet banking has given criminals an opportunity to commit crimes. Between 2015 and 2017, cyber breaches on security targeting financial institutions increased by 30%. This reinforces the assertion that financial service institutions are 300 more times prone to be victims of cyber-security compared to other businesses. Nigeria is a leading country in cyber-crime and the landscape is ever transforming as more sophisticated attacks keep emerging. The banking sector in Nigeria face cyber-security threats which have become a major threat to the sector. Viruses, worms, and hacking are the common types. Phishing, online fraud, and fake-cat websites are also experienced in the sector (Wang, Nnaji and Jung, 2020).

In Kenya reports indicate there is an evolving cyber-security landscape which shows there is a web of sophisticated insiders and outsiders who have been launching frequent and targeted cyber-attacks. Standard to detect and response to incidences are complicated by the increasing sophistication. Insider threat was as of 2013 the biggest threat as organisation employees. PBX fraud/hacking was also commonly used to target organisations. Other common cyber-crimes include the Denial of Service (DoS) where attackers deny users services; Botnet attacks where compromised computers are deployed; online & mobile banking attacks; mobile money fraud; and cyber espionage where data is stolen from systems of organisations (Kigen et al., 2014).

Apart from attacks on organisations and governments the private sector in Kenya has experienced cyber-attacks. Banks and other financial institutions such as MFI have lost millions of shillings. Barclays bank in 2019 lost KES 11 million through its ATMs. Such trends led to the CBKs Cyber-security Guideline for Payment Service Providers (Munyori and Mumbi, 2020). As indicated by Serianu (2018) over 90% of cyber-crime cases go unreported and therefore, the reported costs are just estimations. Indirect costs associated with cyber-crimes in financial services are estimated to be KES 64 million. These are costs associated with antivirus, insurance and compliance costs. The direct costs on financial service providers is estimated to be KES 28 million which includes lost money, hijacked data (ransomware), fines and other costs.

2.2 Cyber-security Strategies, Policies and Legal Frameworks

In Europe the Council of Europe (CoE) Convention was put in place to repress cyber-crime. Apart from harmonizing the definition of cyber-crime, the Convention introduces tools to investigate and introduces a framework for cooperation among European states. this Convention is hailed as critical in the international fight against cyber-crime. There are however reservations on the implementation of such international frameworks. This might limit its effectiveness (Calderoni, 2010).

The financial sector has developed regulations to address the increasing cases of cyber-crime. Financial institutions have taken diverse measures. In Ghana the Bank of Ghana developed a cyber-security directive that required formation of a Cyber and Information Security Office which is charged with advising and formulating measures. In Nigeria, the Central Bank of Nigeria developed a risk based cyber-security framework for financial institutions. In Kenya, the Central Bank made Cyber-security policies mandatory (Kshetri, 2019).

Financial fraud is one of the many cyber-criminal threats Africa faces due to lack of proper protection. In the East Africa region efforts to combat cybercrime have taken a multi-stakeholder approach. There is also a regional Task force for dealing with legal, policy and regulations that root out cyber-crime. The five countries in the East Africa region had planned to set up a Computer Emergency Response Team (CERT) in the region. This was to be supported by the International Telecommunications Union (ITU) through the East African Communications Organisation and later to be cascaded into national CERTs. Even though the countries were in

different stages of formulating their national legal frameworks, uniformity in the legal frameworks was to be achieved with few peculiar aspects that characterize each country. In the West of Africa, ECOWAS has been on the front to build the capacities of countries and develop networks to fight cyber-crime. However, the legal, policy and infrastructural loopholes make the fight a bitter one (Quarshire and Martin-Odoom, 2012).

In Nigeria, which is a notorious cyber-crime hub, cyber-crime is being fought through various facets. The Economic and Financial Crime Commission (EFCC), the Nigeria Police Force and a National Security Adviser are involved in the fight against cyber-crime. In addition critical institutions, the Nigeria Communications Commission, National Intelligence, Department of State Service, and Nigeria Computer Society are also involved. A Cyber-crime Bill was introduced and passed. Other institutions created to tackle cyber-crime were the Directorate of Cyber Security and the Crime Prosecution Unit. These magnitudes of institutions and legal frameworks are testament to the cyber-criminal levels in Nigeria (Ummar-Ajijola, 2011).

South Africa has put in place strategies, policies and regulatory frameworks for countering cyber-crime. The country has among others, a Cyber-security Policy, National e-Strategy and National Cyber-security Policy Framework. Kenya has managed to also put in place measures that include the National Cyber-security Strategy of 2014; National Cyber-security Master Plan; National Cyber-security Framework of 2014; and the Kenyan Information and Communications Technology Policy, 2006. Other frameworks which have clauses touching on Cyber-security and cyber-crime are the Kenya's National Security Intelligence Service Act 11 of 1998; Cyber-security and Protection Bill 2016; Computer and Cybercrimes Bill 2016; Critical Infrastructure Protection Bill; and the Data Protection Bill 2015 (Gumbi, 2018).

The U.S has some of the most elaborate and diverse strategies, policies and regulatory frameworks. In number, the U.S also has numerous of such frameworks. To mention a few, there is the Computer Fraud and Abuse Act of 1986; Cyber-security Information Sharing Act of 2015; Cyber Security Enhancement Act of 2002; Cyber Research and Development Act of 2002; and the Homeland Securities Act of 2002. The U.K has a range of strategies, policies and regulatory frameworks such as the National Cyber Security Strategy, Computer Misuse Act of 1990, Network and Information Security Directive and the General Data Protection Regulation. In

India, there is, among other, the State Cyber Security Policy of 2016 in Telangana state and the National Cyber Security Policy of 2013. Even though these strategies, policies and regulatory frameworks have helped manage cyber-crime, the unique features of cyber-crime have made existing laws and frameworks less effective in prosecutions. The laws have also not kept up with the fast evolving nature of cyber-crime (Gumbi, 2018).

As cyber-attacks and threats continue to become severe and more complex industries adopt various measures. One is the Security Information and Event Management Tools (SIEM) that has become critical in the financial sector. The Web Application Firewall (WAF) that secures web application is also being implemented to secure internet banking. To address the Credit/Debit card fraud/theft, banks have shifted to chip-based technology from the magnetic strip cards which were prone to skimming. In addition to these sector wide measures, there are regional and national efforts. Regionally, Common Market for Eastern and Southern Africa (COMESA) has developed a Cyber Security Program for public-private partnership in matters of cyber-security. This enhances networks and cyber-security platforms. In Kenya, the Cyber Security Master Plan (CSMP) addresses issues of training and awareness creation. The Kenya Computer Security and Incident Response Team (KE-CSIRT) addresses the safety angle of the cyber environment. The Cyber-crime Bill and the Kenya Information and Communication Bill of 2013 have helped in defining and laying down clear structures that enable prosecution of cyber-crime (Kigen et al., 2014).

Still on Kenya Munyori and Mumbi (2020) show that cyber security is governed by a range of provisions. The Constitution of Kenya 2010 Article 31; Kenya Information and Communication Act No. 2 of 1998; the Data Protection Act No. 24 of 2019 and the Computer Misuse and Cyber Crimes Act No. 5 of 2018 are some of the legal frameworks addressing cyber-crime.

CHAPTER THREE

DATA ANALYSIS, PRESENTATION, DISCUSSION

3.0 Introduction

This chapter is composed of an analysis of the data which was gathered during field work. This data is presented in form of graphs, tables and charts. The data is also presented using prose form. Lastly, the chapter discusses the findings and compares these findings to published literature that anchored the study.

3.1 Response Rate

The researcher conducted field work from the month of October to the month of December, 2022. First, the researcher contacted the financial institutions and physically took questionnaires to the banks and microfinance institutions. The researcher requested that the questionnaires should be filled by the relevant department (Fraud, Security or top management) within three weeks. Secondly, the researcher contacted the BFIU, FRC, and private cyber security firms. Interview dates were scheduled based on the availability of the respondents. Interview notes were taken during these face to face interviews. Based on reference from one of the experts, the researcher was directed to interview the Communications Authority of Kenya as this government agency is in charge of development and management of Cyber-security frameworks in Kenya.

From the methodology in chapter one, this study indicated that 50 questionnaires will be filled by banks (domestic and foreign) and MFIs while five interviews would be conducted with the BFIU, FRC and private Cyber security firms based in Nairobi County. From this proposed numbers, this study sent questionnaires to 50 financial institutions in Nairobi County. From these 50 questionnaires, 30 questionnaires were successfully filled and returned. This is a return rate of 60%. The other 20 questionnaires were not filled by the respondents as the targeted financial institutions refused to participate, failed to meet the deadline and others stated the topic of the study was very sensitive for them to respond.

In addition to these questionnaires, 4 interviews were conducted. Institutions that were interviewed included the BFIU, Communications Authority of Kenya and two cyber-security companies. The other interviews failed to materialize as respondents were unwilling to participate while others had busy schedules and could not find time.

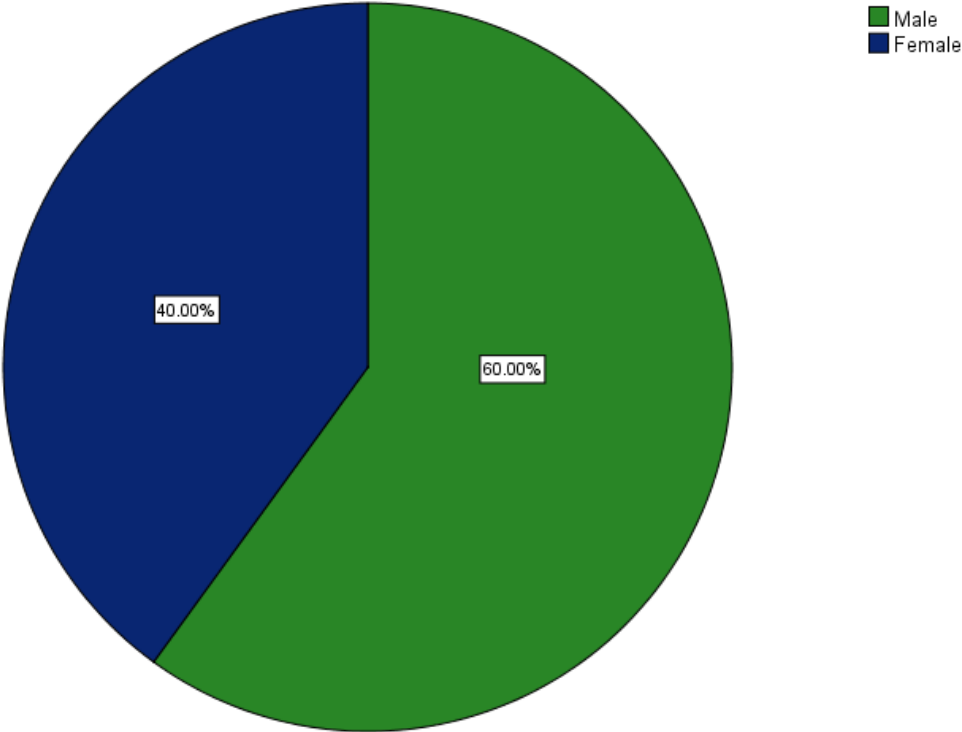
3.2 Respondent Demographic Information

This section will outline the characteristics of the respondents. Information ranging from gender, age, education and type of financial institution they work in will be outlined.

3.2.1 Gender

Findings show that 60% of respondents were male and 40% were female. As shown in the pie chart below, there were more male respondents than female respondents in the financial institutions that took part in this study.

Figure 1: Respondent Gender



Source: Field Research (2022)

3.2.2 Age of Respondent

Respondents were required to indicate their age. From the findings 53.3% of respondents were within the 26-35 years age bracket, 33.3% were within the 36-45 years age bracket and 13.3% were in the 46-55 years age bracket. This shows that majority of the workforce from the financial institutions that responded to this study were between the ages of 26 and 35 years of age. This is shown in the table below.

Table 1: Respondents Age Bracket

Age bracket	Frequency	Percent
26-35 years	16	53.3
36-45 years	10	33.3
46-55 years	4	13.3
Total	30	100

Source: Field Research (2022)

3.2.3 Respondent Level of Education

Findings on the respondent's education shows that 80% of participants were graduates and 20% had post graduate level of education. This shows that majority of respondents had at least graduate level education.

Table 2: Respondents Level of Education

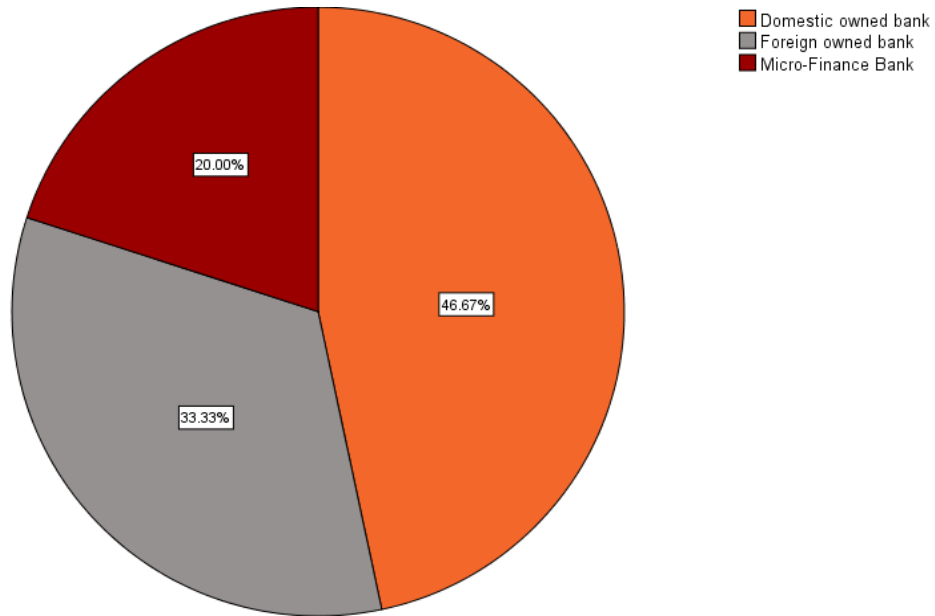
Education	Frequency	Percent
Post-graduate	6	20.0
Graduate	24	80.0
Total	30	100

Source: Field Research (2022)

3.2.4 Type of Financial Institution

On the financial institutions that participated in this study, findings show that 46.67% were Domestic owned bank, 33.33% were Foreign owned banks and 20% Micro-Finance Institutions. This finding shows that majority of respondents were from domestically owned banks. This finding is representative of the actual situation as there are more domestic owned banks in Kenya.

Figure 2: Financial Institution



Source: Field Research (2022)

3.3 Financial Impacts of Cybercrimes on the Banking Sector

Findings show there are a range of Cyber-crimes that affect the Banking Sector. From the findings, 60% of participants indicated that the most common group of cyber-crimes are Hacking, Identity theft, Electronic card fraud, Card info skimming, and Mobile banking breaches. This was followed by Hacking, Malware, Phishing, Mobile banking breaches at 20% and lastly, Hacking, Electronic card fraud, Phishing, Card info skimming, and Mobile banking breaches at 20%. Though respondents were allowed to tick multiple responses in this question, it is evident that the most common cyber-crimes are Hacking and Mobile banking breaches which were mentioned in all the three distinct groups. Interview findings show that hacking to steal data, identity theft through email compromise or account take over, SIM-swap and collusion with staff are the major cyber security threats. However, it was evident that the most lucrative end goal is taking over control of the banking system. This is the ultimate cyber-crime as the ‘rewards’ as considered immense by cyber criminals. From interviews conducted, phishing and

related crimes are on a decline as they do not give direct monetary rewards. A respondent verbally indicated that:

Banks, microfinance institutions and SACCOS have areas commonly targeted for attack by cyber-criminals. ATM infrastructure compromise, mobile banking infrastructure, debit and credit card systems, third parties and vendors and identity management systems compromise which are all targeted for fraud (KII 4, 15 December, 2022).

Table 3: Type of Cyber-crimes

Cyber-crime	Frequency	Percent
Hacking, Malware, Phishing, Mobile banking breaches.	6	20.0
Hacking, Identity theft, Electronic card fraud, Card info skimming, Mobile banking breaches.	18	60.0
Hacking, electronic card fraud, Phishing, Card info skimming, Mobile banking breaches	6	20.0
Total	30	100

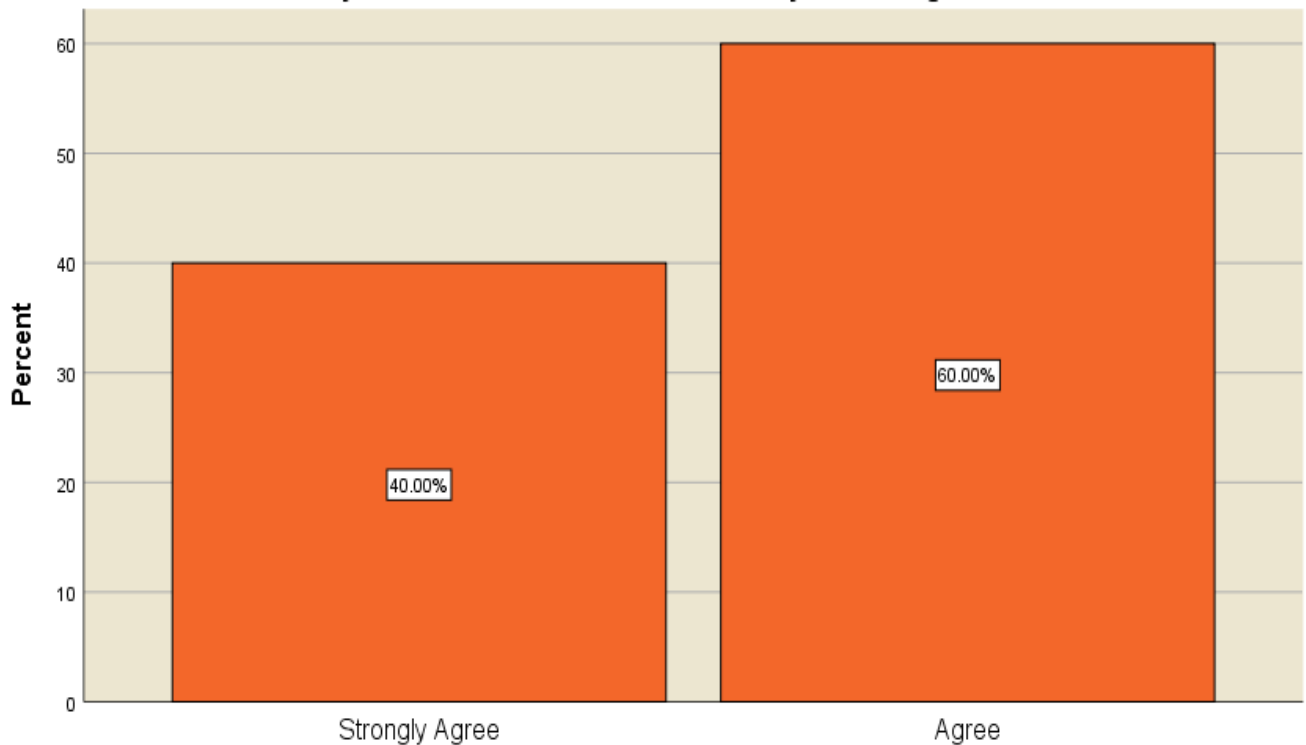
Source: Field Research (2022)

In relation to the above, studies such as that of CA (2021) showed that cyber threats in Kenya have increased due to technological advancement which creates opportunities for cyber-crime. Malware such as ransomware is a common type. Additionally, Wasuna (2021) highlights some of the crimes. This study relates to the current findings in that it showed that cyber-crime involved recruiting of internal bank staff which was revealed at Equity Bank in Kigali, Rwanda where cyber-criminals with intent to commit a cyber-attack were caught recruiting bank staff. The current findings also relate with previous studies including the findings of Agrawal (2016) who found that cyber-attacks are prevalent in banks information systems, transactional systems, ATMs, credit card and debit cards, internet banking, and mobile banking. In the study some of the prevalent cyber-crimes in the banking sector were hacking, credit card fraud, phishing, spyware, key-logging, viruses, watering-hole, credit card redirection and malware attacks. The

current study however, did not find watering-hole to be a key cyber-crime. Additionally, Oliveira and Stickings (2016) showed that recently financial institutions report more incidences of cybercrime more than any other crime. Financial institutions face cybercrimes that include hacking and DoS attacks. Other types of cyber-crime include robbery and fraud which are facilitated by technology.

On whether Cyber-crime has a financial cost on financial institutions, findings show that 60% of participants Agreed and 40% of participants Strongly agreed. This is a strong indication that participants totally agree cyber-crime has a financial cost to financial institutions. Interview findings showed that the financial costs are very huge. These costs are composed of bank cash losses and compensation to the clients who have lost finances. Further to this, these costs include the fines by the CBK which are charged as punishment for not following the required regulations.

Figure 3: Cyber-crime has a Financial Cost on Financial Institutions



Source: Field Research (2022)

On the estimated annual financial losses experienced by financial institutions because of Cyber-crime, findings show 50% of financial institutions have suffered between 1,000,000 and 10,000,000 million Kenya shillings; 33.3% of financial institutions have lost between 11,000,000 and 30,000,000 million Kenya shillings and lastly, 16.7% of financial institutions have suffered between 100,000 and 800,000 Kenya shillings. This is an indication that majority of the financial institutions have lost between one million and ten million Kenya shillings. This is shown in the table below.

Table 4: Estimated Annual Financial Losses

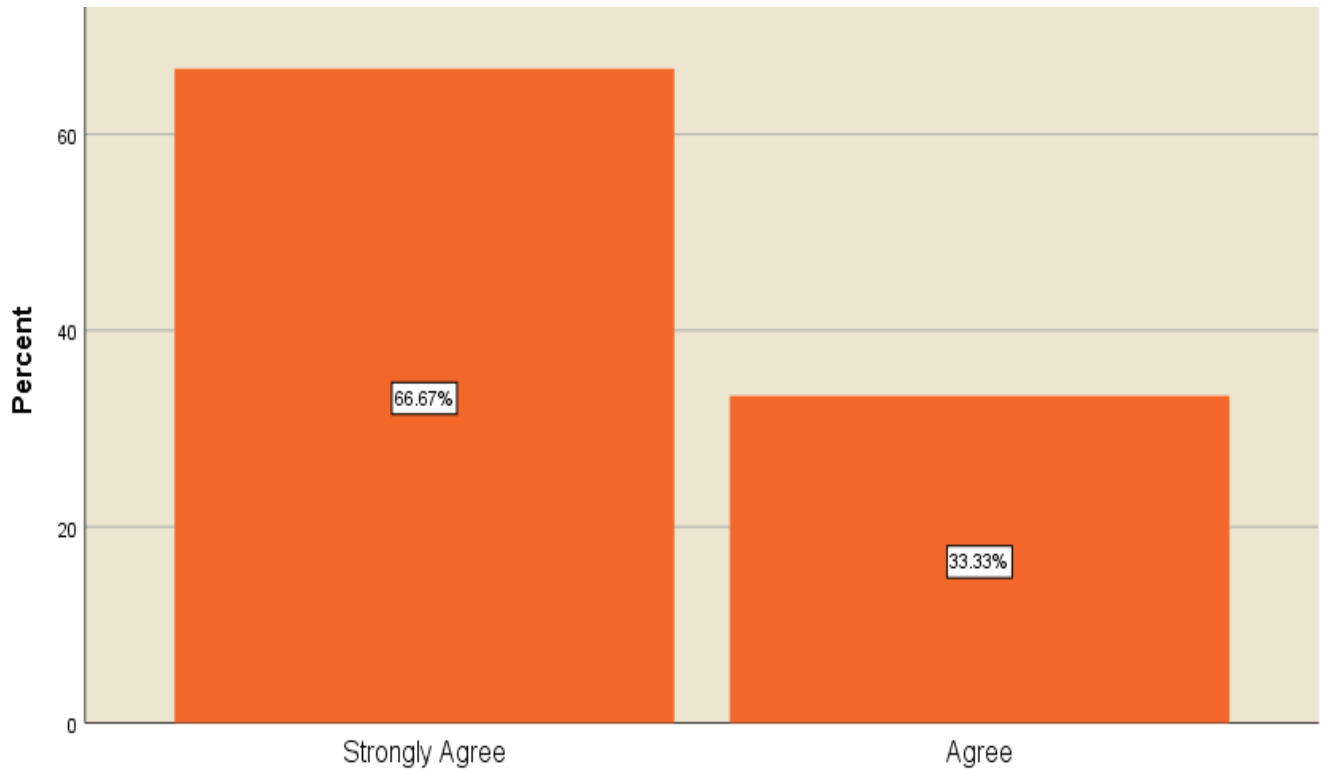
Financial Losses	Frequency	Percent
100,000 - 800,000	5	16.7
1,000,000 – 10,000,000	15	50.0
11,000,000 – 30,000,000	10	33.3
Total	30	100

Source: Field Research (2022)

In addition to these findings, interviews noted that financial losses in the banking sector were in the hundreds of thousands running into several billions. Such losses are an indication that losses are colossal. There was however concerns that banks do not reveal some of the cyber-crime cases to the CBK as required by regulations which is an illegality. Secondly, banks tend to underreport the real figures of lost finances as this is a reputational risk. Therefore, the figures normally presented by banks may not be accurate.

Findings on the costs of countering cybercrime show that 66.67% of participants Strongly agreed and 33.33% of participants Agreed that there are high costs used for countering cybercrime activities by financial institutions. There were no other responses given by the respondents. This findings show that majority of participants strongly feel there are high financial costs that come with countering Cyber-crime in the financial sector.

Figure 4: Countering Cybercrime Activities in the Banking Sector has a High Cost



Source: Field Research (2022)

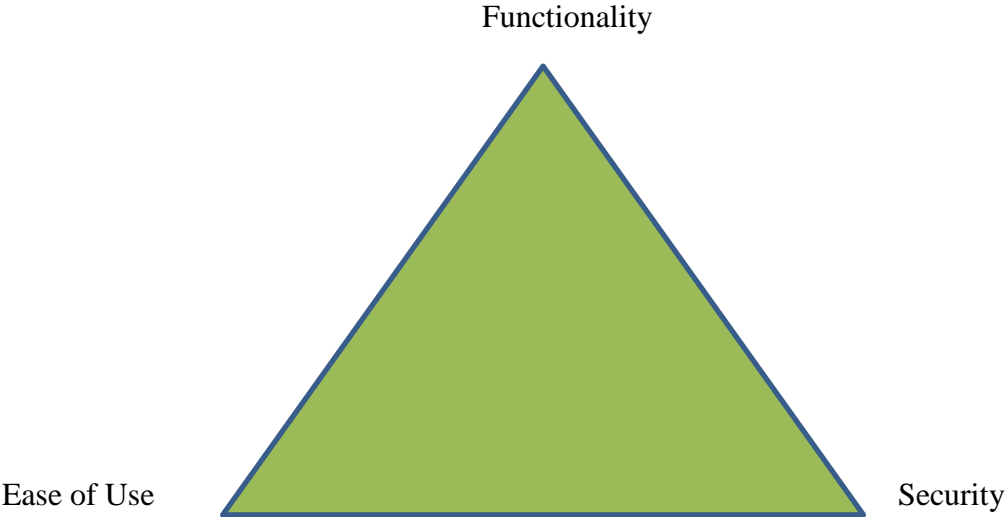
Interviews revealed that the cost of cyber-security is very high. It is a large percentage of the annual bank profits and this makes banks to invest less in security systems as they try to maximize profits. Cyber-security infrastructure/software and personnel are expensive which deters banks from investing in extra cyber security beyond the sector required threshold. As indicated by an interviewee:

Bank systems will always be attacked by cybercriminals. Tier 1 banks and Tier 2 banks together with the smaller banks all have lower measures put in place. This is because the systems and processes in cyber-crime are capital intense. These banks are therefore always on the radar of criminals (KII 2, 8 December, 2022).

In another dimension, a bank investment in cyber-security is also tied to functionality of their services and ease of use of bank services by clients. This multi-pronged interconnection creates a dilemma for financial institutions. The functionality of banking apps and systems should

guarantee ease of use by clients. However, this may introduce security risks. Therefore, increased functionality guarantees the ease of use which increases insecurity in certain bank applications and/or systems. This interconnection leads banks to try and attain a balance on security to ensure high functionality and smooth ease of use by clients. This shown in the diagram below:

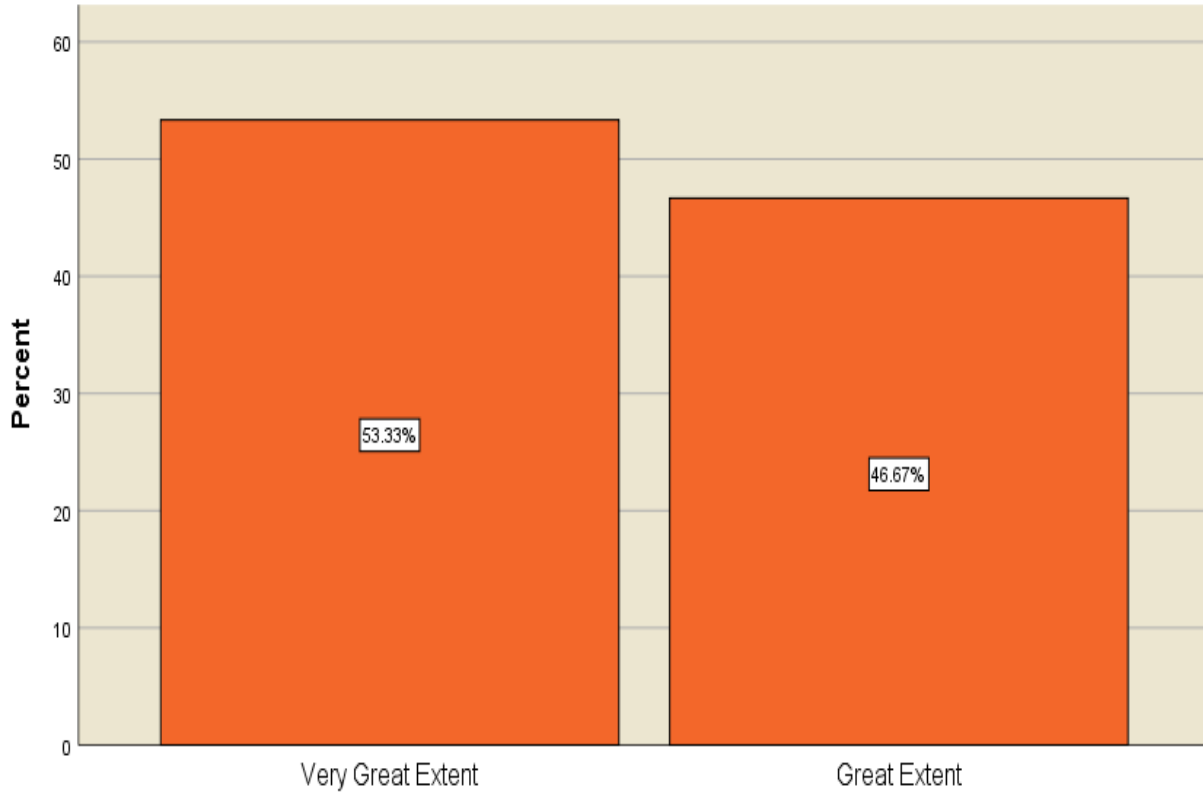
Figure 5: Logic of Cyber-security Investment by Financial Institutions



Source: Field Research (2022)

On the impact of cyber-crime on Foreign Direct Investment in the banking sector, findings show that 53.33% of participants stated it impacted FDI to a Very great extent and 46.67% stated it affected FDI to a Great extent. This shows that majority of the participants agreed that cyber-crime negatively impacted financial institutions.

Figure 6: Extent of Effects of Cybercrime on FDI in the Banking Sector



Source: Field Research (2022)

3.4 Impacts of Cybercrimes on Bank data in the Banking Sector

On the common types of data targeted cyber-crimes in financial institutions, findings show that a combination of Ransomware, Phishing and Denial of Service are the highest at 33.3%. This is followed by Ransomware at 26.7%; Ransomware, Malware and Phishing at 20% and Ransomware and Phishing at 20%. Even though a combination of Ransomware, Phishing and Denial of Service are the most prominent in the financial sector it is evident from the findings that Ransomware and Phishing are also very common as they were independently mentioned by all the groups as shown in the table below.

Table 5: Common Types of Data Targeted Cyberattacks

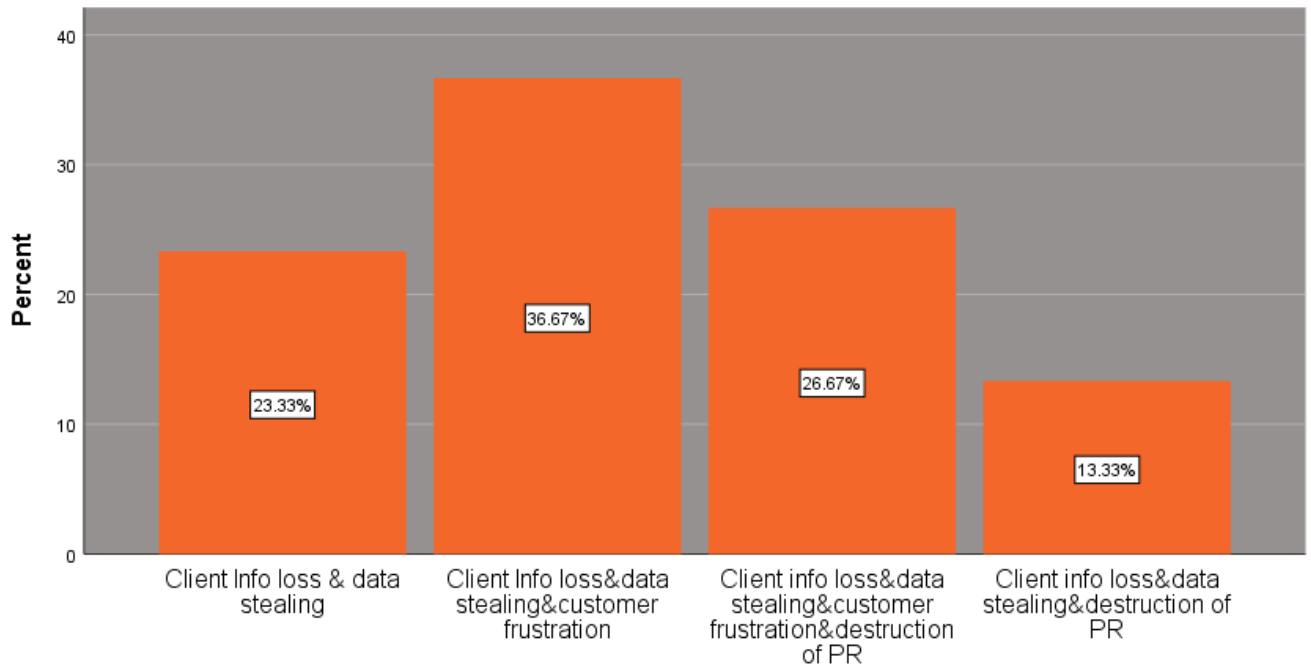
Data Cyberattacks	Frequency	Percent
Ransomware	8	26.7
Ransomware, Malware and Phishing	6	20.0
Ransomware, Phishing and Denial of Service	10	33.3
Ransomware and Phishing	6	20.0
Total	30	100

Source: Field Research (2022)

Interview findings show that within the banking sector other data targeted cyber-attacks is Business Email Compromise (BEC) which is also referred to as Email Account Compromise (EAC). This is exploited by cybercriminals to impersonate and defraud banks or other companies doing business with the banks. In this type of cyber-crime, criminals impersonate personnel with authority to effect payments or ones who are supposed to receive a payment. This normally takes place over email communication and results in financial transactions to fraudulent accounts. Previous studies have a relation to some the current findings. CA (2017) indicated that botnet attacks, malware, phishing, virus attacks, disclosure of personal information e.g. PINS and passwords through duping and hacking of technical infrastructure are some of the cyber-crimes prevalent in Kenya.

Among the types of data losses from cyber-attacks, findings show that 36.67% were Client information loss, data stealing and customer frustration; 26.67% was Client information loss, data stealing, customer frustration and destruction of PR; 23.33% was Client information loss and data stealing; and lastly, 13.33% was Client information loss, data stealing and destruction of PR. This also shows that Client information loss and data stealing are dominant types of losses common within banking institutions as shown in the bar chart below.

Figure 7: Types of Data Losses from Cyber-crimes



Source: Field Research (2022)

On the extent of the negative impact of cyber-crime due to data losses, findings show that 40% of participants stated that the negative effects were to a Very great extent and 60% stated it was to a great extent. This shows that majority of respondents feel that cyber-crime targeting data has a negative effect on the banking sector.

Table 6: Extent of negative impact from data loss cyber-attacks on Kenya's banking sector

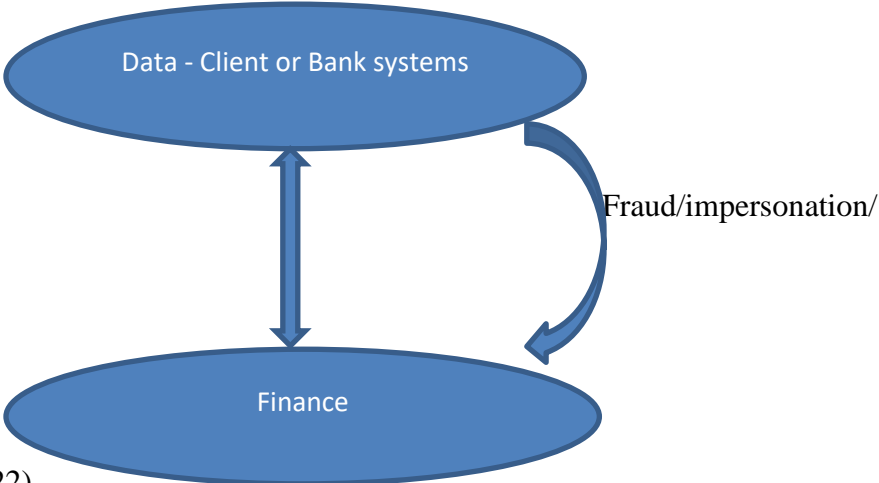
Response	Frequency	Percent
Very great extent	12	40.0
Great extent	18	60.0
Total	30	100

Source: Field Research (2022)

The findings from the key informant interviews reveal that loss in data can be an independent cyber-attack but it can also be related to financial losses. Some cyber-attacks target bank data or client personal data as an end but in other cases data is meant to lead to attacks targeting finance.

Finance and data are therefore, in a way interconnected or mutually reinforcing in the latter case. Expert interviewees revealed that loss of data leads to financial losses. The data stolen from banks can be information on clients or bank systems. This data is at times sold in the dark web to hackers who understand how to use it. Such data can be used to infiltrate a financial institution or can be used to impersonate a client leading to financial losses. This relation between cyber-attacks targeting data only or those targeting data for financial ends is shown in the figure below.

Figure 8: Relation between Finance and Data losses



Source: Field Research (2022)

3.5 Cyber Security Measures put in place by the Banking Sector

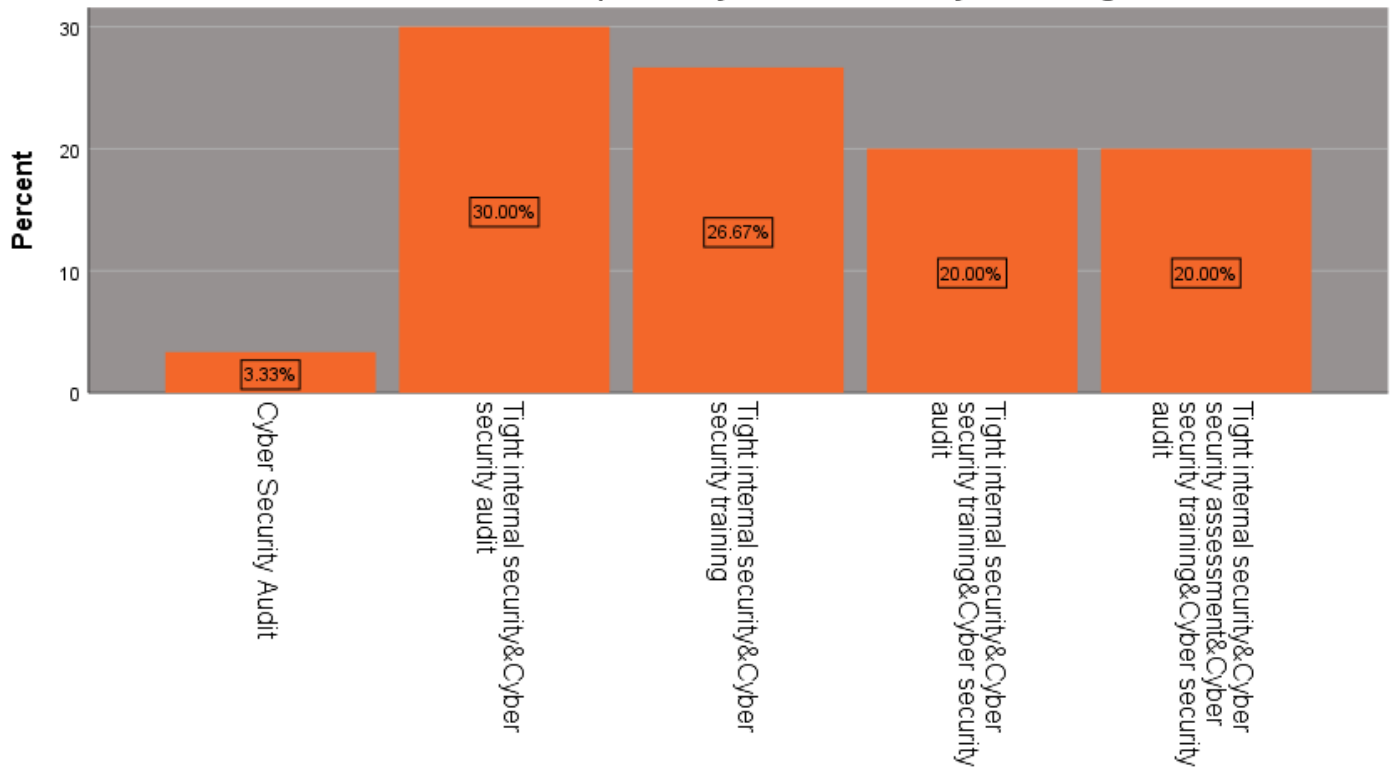
Financial institutions that participated in this study have put cyber-security measures in place to target and solve cyber-crimes. Among the cyber security measures mentioned by participants are use of advanced and protected banking softwares; using online and offline security applications such as antivirus; having personalized accounts with passwords/login key; and having a limited access feature within the banking software system. Other measures put in place include consistent training of the bank employees on issues of cyber-crime and cyber security.

Findings from the interviews show that banks and MFIs have developed several strategies over the years. These strategies are also updated as new threats emerge. First, financial institutions have enacted the Know Your Customer (KYC) standard where institutions establish customer identity through physical contact. Secondly there is the One Time Password (OTP) feature which

is a systems security SMS feature sent to clients via phones for verification of transactions. The other strategies target the financial institutions staff. Staffs are vetted and are given access controls according to their management level. This is meant to make sure only a credible staff are employed and also make sure the staff can only access information as per their 'pay grade'. This is also referred to as access control rights. Lastly, banks and MFIs vet the software vending companies (Third party vendors) to ensure that any software procured is genuine and does not have backdoors that can be exploited by cyber-criminals. However, not all banks comply with such measures. In light of the training done by financial institutions, the current study speaks to past studies. Staal (2015) had found that financial institutions remain unaware and their personnel are ill-equipped to detect or even identify threats till the crime has been committed. This signals the importance of the ongoing training and the need for further training. However, Mugari (2016) found that in trying to prevent the challenge of cyber-crime, financial institutions have resulted to training, updating softwares and firewalls.

On the methods used by financial institutions to prevent cyber-attacks, respondents gave a combination of measures as used by financial institutions. Findings show that 30% of respondents stated Tight Internal Security & Cyber Security Audit were the most common methods. Another 26.67% stated Tight Internal Security & Cyber Security Training; 20% stated that Tight Internal Security & Cyber Security Training & Cyber Security Audit; another 20% stated that all measures, that is, Tight Internal Security & Cyber Security Assessment & Cyber Security Training & Cyber Security Audit were used. Lastly 3.33% stated that Cyber Security Audit was the main measure. This is shown in the bar chart below.

Figure 9: Measures used to Prevent Cyber-crime in the Banking Sector



Source: Field Research (2022)

Interview findings are in sync with some of the findings from the questionnaires. As noted by participants banks and MFIs have put in place training programs that continually improve the skill set and knowledge of their security as well as administrative staff. However, it was noted that the trainings are not adequate. They are few and far between. This was noted by the participant below:

Banks have training programs that enhance cyber-security know-how and reporting. The only problem is that we who do that training know banks do not do as much as we recommend. There are a lot of complex things which need to be taught several times over. Other technical issues require refresher courses which banks are never interested in (KII 4, 15 December, 2022).

In terms of the extent to which the above measures used in the banking sector have prevented Cyber-attacks, findings show that 53.3% stated to a Moderate extent, 26.7% stated to a Very great extent and 20% stated to a Great extent. No other responses were given by the participants.

This shows that majority of the participants from banks and MFIs have moderate confidence in the Cyber-security measures as shown in table below.

Table 7: Extent to which Existing Cyber-security Measures Prevent Cyber-attacks in Kenya's Banking Sector

Response	Frequency	Percent
Very great extent	8	26.7
Great extent	6	20.0
Moderate extent	16	53.3
Total	30	100

Source: Field Research (2022)

The above findings were also revealed by the interview findings. Majority of participants indicated that banks do not take cyber-security as important as they should. Cyber-security as a high priority issue does not get the necessary attention that it should. Even though there are cyber-security measures they are not adequately resourced or implemented such as the case for trainings. In addition, findings show that financial institutions do not prioritize cyber-security professionals as not all banks have integrated such personnel as permanent staff into the banking system. Cyber-security experts are called on ad hoc basis or meet periodically with bank security and management teams for audit and advice. This was conveyed by an interviewee who noted that:

There is low cyber-security investment by banks. This is an issue that is also tied to the profits banks have to make. But the sensitivity with which cyber-security requires is not an issue banks care about (KII 2, 8 December, 2022).

The above findings also make sense in light of some of the older studies. For instance Symantec White Paper (2015) showed that as financial institutions take advantage of new innovations such as mobile, cloud and other technical trends to meet customer needs, such innovations increase risk as cyber criminals capitalize on this technology to launch attacks. Financial organizations are fighting multiple fronts as financial cyber attackers have become organized and sophisticated.

On the extent to which the current Cyber-security measures used in the sector are by-passed and infringed by Cyber-criminals, 73.3% of participants stated to a Moderate extent and 26.7% stated to a Little extent.

Table 8: Extent to which Cyber-criminals By-pass Existing Security Measures in Kenya's Banking Sector

Response	Frequency	Percent
Moderate extent	22	73.3
Little extent	8	26.7
Total	30	100

Source: Field Research (2022)

3.6 Challenges facing cyber security measures utilized by the banking sector

In terms of the satisfaction levels of financial institutions with regards to the ability of regulatory institutions to implement cyber-crime prevention measures, findings show that 53.3% of participants were Neither satisfied nor dissatisfied and 46.7% were satisfied. There were no other responses from the participants.

Table 9: Satisfaction with Regulatory Institutions Ability to Implement Cybercrime Prevention Measures in the Banking Sector

Response	Frequency	Percent
Neither satisfied nor dissatisfied	16	53.3
Satisfied	14	46.7
Total	30	100

Source: Field Research (2022)

This study asked participants to what extent the state legal frameworks cover cyber-crime related issues in the banking sector. Findings show that 60% of participants stated to a Little extent and 40% stated to a moderate extent.

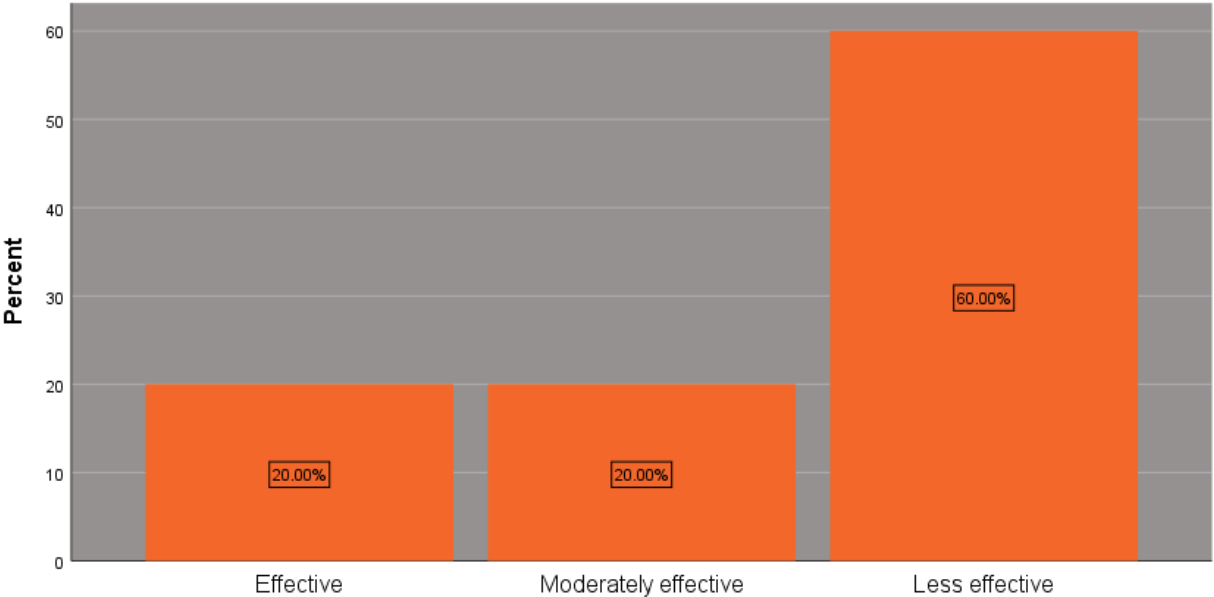
Table 10: Extent to which state legal frameworks cover cybercrime related issues in the banking sector

Response	Frequency	Percent
Neither satisfied nor dissatisfied	12	40.0
Satisfied	18	60.0
Total	30	100

Source: Field Research (2022)

The researcher wanted to understand how effective the Cyber-security legal frameworks are in terms of prosecuting and convicting cyber-criminals. Findings show that 60% of participants stated the legal frameworks are Less effective, 20% stated they are Moderately effective and another 20% also showed they were effective in prosecuting and convicting cyber-criminals.

Figure 10: Effectiveness of Current Cyber-security Legal Frameworks in Prosecuting and Convicting Cyber Criminals



Source: Field Research (2022)

In terms of the effectiveness of the banking sector cyber-security measures put in place to fight cyber-crime, findings show that 46.7% of participants stated the measures are Less effective, 33.3% stated the measures are Moderately effective and 20% stated the measures are effective.

Table 11: Effectiveness of Banking Sector Cyber Security Measures for Fighting Cyber-crime

Response	Frequency	Percent
Effective	6	20.0
Moderately effective	10	33.3
Less effective	14	46.7
Total	30	100

Source: Field Research (2022)

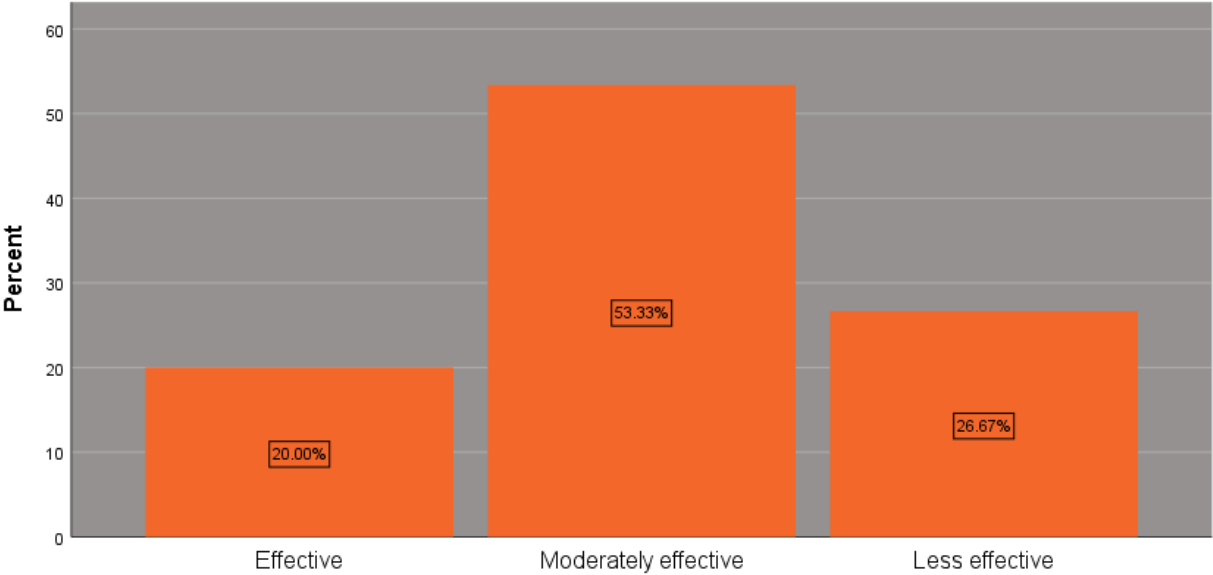
The above finding relates to the findings of Raghavan and Parthiban (2014) who had found that technological enhancements increase fraud and billions of dollars have been lost in the process. Their study established that the factors why some financial institutions are targeted more than others is due to their level of security on authentication systems and their money transfer policies. This finding indicates that similar to the current study, cyber-security measures are weak. Additionally, Vijayalakshmi, Priyadarshini and Umamaheswari (2021) is also relevant as it the most common crimes are not well identified and protected against. The cyber-security measures put in place by the banks are most at times outdated and the process of tracking criminals is time consuming.

Lastly, the study findings show that 53.3% of participants are of the view that regional cooperation mechanisms used in the fight against cyber-crime are Moderately effective, 26.7% though they were Less effective and 20% thought they were Effective. This is shown in the bar graph below. The interview findings show that regional mechanisms have been fair in the fight against cyber-crime. Through several frameworks such as the Mutual Legal Assistance (MLA) treaties and agreements that are handled through the Office of the Attorney General, cooperation and reciprocity with neighbouring countries has yielded some results. These MLAs provide opportunities for international cooperation around matters that are deemed to be cyber-crime.

Through this framework, Kenya has collaborated with countries in Europe and the East Africa Community region to investigate and prosecute cases related to cyber-crime. Such progress is important based on the increasing regional cyber-crime cases as noted by an interviewee who stated that:

We have also documented that regionally coordinated attacks are increasing. Replication of attacks in East Africa regions is an emerging trend. The attacks which are executed, the tolls used and systems which are targeted have taken a regional dimension (KII 4, 15 December, 2022).

Figure 11: Effectiveness of Regional Cooperation Mechanisms in the Fight against Cyber-crime in East Africa region



Source: Field Research (2022)

From interview findings other challenges that threaten the measures put in place were revealed. First, there is a lax environment within financial institutions when it comes to implementing the banking sector cyber-security regulations as required by the CBK. Banks are caught at a crossroads when it comes to on one hand, having stringent cyber-security measures and on the other hand achieving their target profits and maximizing on effective usage of banking services. This has led to some financial institutions being slow to enact the stringent cyber-security

regulations such as the device pairing strategy which links bank accounts to OTP messages to client phone International Mobile Equipment Identifier (IMEI) numbers. Through this strategy a bank links the IMEI identifier number, unique to every phone, to a client's phone number and their bank account. This reduces the chances of fraudulent transactions in case criminals use a different SIM card, or different phone when committing cyber-crime.

Another challenge prevalent among financial institutions is human interference which is mostly connected to current and past employees. This challenge, known as insider threat, is a high risk as personnel (permanent and temporary) have acted either knowingly, done mistakes or acted with neglect therefore, enabling cyber-crime. Further to this, bank contractors, consultants and third party vendors who sell software, hardware or provide a service and have access to the banking systems are a huge threat. This was noted by an interviewee who stated that:

Today the banking sector has to be extra careful with people such as past employees who resigned or were sacked. These people are aware of what to do are and a key menace in cyber-crime. Also the Third Party Vendors who sell bank systems and firewalls etc. they can infiltrate and commit crimes against banks and this is a common thin as most banks are now using similar vendors who have in the past been infiltrated by cyber-criminals (KII 2, 8 December, 2022).

The lack of advanced cyber security measures particularly by the small financial institutions is a sector challenge towards fighting cyber-crime in Kenya. The findings show that small MFIs and small banks lack the financial capacity to invest in cyber-security frameworks and systems or in case they have done so, they have invested in cheaper options or take a long time to upgrade to the new systems. This downside favors the ever-changing character of cyber-criminals who tirelessly work towards system infiltration and exploitation. This challenge is tied to high costs incurred for cyber-security frameworks and high costs of cyber-crime insurance. As indicated, cyber-crime insurance is an expensive undertaking and few financial institutions have managed to adequately cover this operational expense. The current findings should also borrow from Camillo (2017) who recommended cyber intelligence. He further noted that financial institutions should develop and maintain effective information security programs; use data encryption tools and secure their networks; and they should acquire and install sophisticated systems to manage

cyber security risks. Additionally, the expensive nature of cyber-security is highlighted by Petterson (2012) who found that cyber-security is not a one size fits all solution as evolution of technology shows threats and vulnerabilities are also varied. Malicious attacks are not only catching up with the security but they now cost more to financial institutions.

Another challenge emerging from the interview findings shows that data protection audits, cyber-security audits and other such as network audits are expensive ventures. Financial institutions lack resources for frequent if not regularly scheduled audits. Audits pertaining to compliance with regulations, policies and procedures require huge technical and financial resources to conduct. Further to this, audits by technical teams on the security status of cyber-security infrastructure have huge financial costs that many at times financial institutions cannot meet. This is especially with the medium and small financial institutions. Such audits are important in determining the security levels and recommending advanced and the latest system improvements based on the ever evolving cyber-security scene. This finding relates to Tariq (2018) who noted that internal security should be tightened; training and cyber security audits should also be done. Also PWC (2014) findings noted that the methods used in cyber-crime are constantly changing and becoming sophisticated. This forces institutions to result to more efforts to address cyber-crime.

Hypothesis testing

This study proposed the hypothesis that *cyber-crime has a negative effect on Kenya's banking sector*. To test this hypothesis, the Chi Square test of association was applied. Two main issues that is data and finance, were used to test the effect while cybercrime was represented by the various types of cybercrimes recorded in the banking sector. From the attached questionnaire, question 5 represented the variable on cyber-crime, question 6 represented finance and question 12 represented data.

Table 12: Chi-Square Tests

Value	Value	Degree of freedom	Asymptotic significance
Pearson Chi-Square	30.000	2	0.000
N of Valid Cases	30	—	

The *p-value* in the “Asymptotic Significance (2-sided)” column which is 0.000 is an indication that the result is significant at the designated standard alpha level 0.05. This indicates that the variables are associated and as cybercrime increases, the negative impact on banks increases. Therefore, we accept the null hypothesis that cyber-crime has a negative effect on the banking sector.

CHAPTER FOUR

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

4.0 Introduction

This chapter summarizes the findings of this study; it gives a conclusion and recommends proposals for the regulatory authorities and financial institutions in Kenya. It concludes by suggesting areas that may be investigated by future studies.

4.1 Summary of Findings

4.1.1 Financial Impacts of Cybercrimes on the Banking Sector

This study found that the most common grouping of cyber-crimes that are recorded by financial institutions are Hacking, Identity theft, Electronic card fraud, Card info skimming, and Mobile banking breaches. In general, Hacking and Mobile banking breaches were the most common cyber-crimes which financial institutions in Kenya are facing. In addition, hacking to steal data, identity theft using email compromise or account take over, SIM-swap and collusion with bank staff are other cyber security threats faced by banks and MFIs. However, it was evident that the most lucrative end goal of cyber-crime is taking over control of the banking system. This is the ultimate cyber-crime as the ‘rewards’ as considered immense by cyber criminals.

Findings show that cyber-crime has a financial cost on banks and MFIs. Majority of participants were in agreement that there are huge costs associated with cyber-attacks. Financial institutions have lost between one million and ten million Kenya shillings. However concerns were raised that banks do not reveal some of the cyber-crime cases to the CBK as required by regulations which is an illegality. Secondly, banks have a tendency to underreport the actual figures of lost finances as this is a reputational risk. Therefore, the figures normally presented by banks may not be accurate.

The costs of establishing and maintaining cyber-security systems and infrastructure are very high. It is a huge percentage of the annual bank profits and this makes banks to invest less in security systems as they try to maximize profits. Cyber-security infrastructure/software and personnel are expensive which deters banks from investing in extra cyber security beyond the sector required threshold. Majority of the participants cited that there is a huge financial

investment when it comes to countering cybercrime activities by financial institutions. Further interrogation of this established that bank investment in cyber-security is tied to functionality of their services and ease of use of bank services by clients. Therefore, increased functionality guarantees the ease of use which increases insecurity in certain bank applications and/or systems. This interconnection leads banks to try and attain a balance on security to ensure high functionality and smooth ease of use by clients.

Lastly, the study found that cyber-crime has negative impact on any foreign direct investments in the banking sector. Majority of participants stated the impacts are negative towards FDI within the banking sector.

4.1.2 Impacts of Cybercrimes on Bank data in the Banking Sector

On the types of data targeted cyber-crimes in financial institutions, findings show that a combination of Ransomware, Phishing and Denial of Service are the most common cyber-crimes targeting data. Generally, Ransomware and Phishing are the most prevalent. In addition, Business Email Compromise (BEC) also referred to as Email Account Compromise (EAC) is also exploited by cybercriminals to impersonate and defraud banks or companies that do business with financial institutions.

This study found that some of the most common bank data losses from cyber-attacks included client information loss, data stealing and customer frustration. Majority of respondents felt that cyber-crime targeting data has a negative effect on the banking sector. Other findings reveal that loss in data can be an independent cyber-attack but it can also be related to financial losses. Some cyber-attacks target bank data or client personal data as an end but in other cases data is meant to lead to attacks targeting finance. Finance and data are therefore, in a way interconnected or mutually reinforcing in the latter case.

4.1.3 Cyber Security Measures put in place by the Banking Sector

This study found that some of the cyber security measures in financial institutions include the use of advanced and protected banking softwares; online and offline security applications such as antivirus; firewalls; personalized accounts with passwords/login key; and a limited access feature/access control rights within the banking software system. Other measures put in place

include consistent training of the bank employees on issues of cyber-crime and cyber security. Financial institutions have also enacted the Know Your Customer (KYC) standard where institutions establish customer identity through physical contact; and One Time Password (OTP) feature is used as a systems security SMS feature sent to clients via phones for verification of transactions.

This study further found that financial institutions vet staffs. The personnel are given access controls according to their management level. This is meant to make sure only credible staff are employed and also make sure the staff can only access information as per their management level. This is also referred to as access control rights. Lastly, not all banks and MFIs vet the software vending companies (Third party vendors) to ensure that any software procured is genuine and does not have backdoors that can be exploited by cyber-criminals.

Financial institutions have put in place several measures to prevent cyber-attacks. There is Tight Internal Security & Cyber Security Audit which are the most common methods. Other measures are Cyber Security Training and Cyber Security Assessment. However, Cyber Security Audit is the main measure. The banks and MFIs have put in place training programs to continually improve the skill set and knowledge of their security personnel as well as administrative staff. However, this study established that these trainings are not adequate as they are few and far between. All the measures used within financial institutions have been able to prevent Cyber-attacks to a moderate extent as cyber-attacks are still reported. This finding found that financial institutions do not take cyber-security as important as they should. Cyber-security is a high priority issue but does not get the necessary attention that it should. Even though there are cyber-security measures they are not adequately resourced or implemented such as the case for cyber-security trainings. In addition, findings show that financial institutions do not prioritize cyber-security professionals as not all banks have integrated such personnel as permanent staff into the banking system. Cyber-security experts are called on ad hoc basis or meet periodically with bank security and management teams for audit and advice.

4.1.4 Challenges facing cyber security measures utilized by the banking sector

There are various challenges relating to cyber-security measures that rock the banking sector. First, financial institutions have low satisfaction levels in the ability of regulatory institutions.

Particularly, financial institutions are not satisfied with the implementation of cyber-crime prevention measures by the regulatory institutions in the sector. Secondly, there are gaps in the state legal frameworks as they do not sufficiently cover cyber-crime related issues in the banking sector. On the level of effectiveness of the legal frameworks, this study found that the cyber-security legal frameworks are also moderately effective in prosecuting and convicting cyber-criminals. Largely, there is moderate confidence in the banking sector cyber-security measures for fighting cyber-crime.

This study also found that the regional cooperation mechanisms for fighting against cyber-crime are moderately effective. The regional mechanisms have been fair in the fight against cyber-crime. Through some of the frameworks such as Mutual Legal Assistance (MLA) treaties and agreements, handled through the Office of the Attorney General, there have been cooperation and reciprocity with neighbouring countries leading to arrests and prosecution of cyber-crime cases.

There is a lax environment in the banking sector when it comes to implementing sector cyber-security regulations by banks and MFIs as required by the regulators such as CBK. Financial institutions are caught at a crossroads when it comes to implementing stringent cyber-security measures and on the other hand, achieving target profits and maximizing on effective usage of banking services. This has led to reluctance by some financial institutions in enacting stringent cyber-security regulations such as device pairing which links bank accounts, OTP messages and client cellphone IMEI numbers.

Another major challenge revealed in this study is human interference. This is connected to current and past employees who pose 'insider threat'. This is high risk as permanent and temporary personnel at times knowingly do mistakes or act with neglect therefore enable cyber-crime. This amounts to collusion with criminals. Bank contractors, consultants and third party vendors in charge of selling software, hardware or provide a service to financial institutions and have access to banking systems may also pose a huge threat.

Lastly, this study found that there is a lack of advanced cyber security measures especially by small financial institutions. This is a sector challenge towards fighting cyber-crime in Kenya.

The findings show that small MFIs and small banks lack the financial capacity to invest in advanced cyber-security frameworks and systems. At times these take a long time to upgrade the available systems they have. There are also high costs associated with cyber-crime insurance in the banking sector. Another area associated with high financial implications is conducting of data protection audits, cyber-security audits and network audits. These are expensive ventures and financial institutions lack resources to conduct frequent and regular audits as required and scheduled. It was revealed that audits pertaining to compliance with regulations, policies and procedures require huge technical and financial resources.

4.2 Conclusion

This study concludes that Hacking, Mobile banking breaches, identity theft using email compromise/account take over, SIM-swap and collusion with bank staff are major cyber security threats that banks and MFIs face. The lucrative end goal of cyber-crime however, taking over control of the banking systems of financial institutions in Kenya.

Cyber-crime has a financial cost on financial institutions. However, Banks and MFIs do not reveal some of the cyber-crime cases to the CBK as required by regulations. Further, the figures presented may not be accurate as financial institutions tend to underreport financial losses emanating from cyber-crime. The study determined that costs associated with establishing and maintaining cyber-security systems and infrastructure is very high. This discourages banks from investing in cyber-security systems as they try to maximize profits. Related to this conclusion is that increase in functionality of banking services guarantees the ease of use therefore, increasing insecurity in certain bank applications and/or systems.

This study concludes that Ransomware, Phishing and Business Email Compromise (BEC)/Email Account Compromise (EAC) are the most common data targeted cyber-crimes. Data losses associated with the mentioned attacks are client information loss, data stealing and customer frustration. Additional conclusion on this is that the data cyber-attacks data can be independent but can also be related to financial losses. Cyber-attacks targeting bank data or client personal data may lead to cyber-attacks targeting finance.

The research concludes that cyber security measures used by financial institutions include use of advanced and protected banking softwares; use of online and offline security applications; use of

personalized accounts with passwords/login key; and use of limited access /access control rights feature. Further financial institutions consistently train their employees; have a Know Your Customer (KYC) standard, and use the One Time Password (OTP) feature that connects to clients cell phones. The financial institutions conduct staff vetting; personnel are restricted through access controls rights and lastly, banks and MFIs vet their Third party vendors to ensure credibility in service and products. We also conclude that financial institutions result to Tight Internal Security, Cyber Security Audit, Cyber Security Assessment and Cyber Security Trainings to safeguard against cyber-attacks.

This study concludes that even with these various measures mentioned, financial institutions have not effectively managed and prevented cyber-attacks. This can be associated with lack of adequate the training for the staff, disregard for the important priority of cyber-security structures, personnel and other resources.

This study further concludes that financial institutions are not satisfied with implementation processes pertaining to cyber-crime prevention measures established by regulatory institutions in the banking sector. The state legal frameworks also have a gap and do not sufficiently cover cyber-crime related issues. This makes prosecuting and convicting cyber-criminals a tall order in some cases. The researcher concludes that regional mechanisms have been fair in the fight against cyber-crime. The Mutual Legal Assistance (MLA) treaties and agreements have aided in cooperation and reciprocity in arrests and prosecution of cyber-crime cases the region.

A lax environment inhibits implementing sector cyber-security regulations within the banking sector. Banks and MFIs have been slow to meet the stringent cyber-security measures as required by the banking sector regulators. Implementation has been at logger heads with achieving target profits and maximizing on functionality of banking services. This study concludes that other challenges are human interference where current and past employees pose an ‘insider threat’; lack of resources to roll-out and keep updating advanced cyber security infrastructure especially by small financial institutions; high financial implications of conducting data protection audits, cyber-security audits and network audits. Lastly, audits on compliance with regulations, policies and procedures have huge technical and financial resources that are at times beyond reach.

4.3 Recommendations

4.3.1 Recommendations for Financial Institutions

This study recommends that the management teams of financial institutions should give cyber-security the attention it deserves. The subordination of cyber-security infrastructure and systems is unwarranted as this has an effect on profits and reputation which are highly valued within the banking sector. The importance of cyber-security should be shown through increased investments towards cyber-security technologies. Constant software and hardware upgrades with the latest and advanced firewalls and antiviruses becoming main investments in by financial institutions. Further, the financial institutions should have dedicated permanent departments and/or personnel with cyber-security expertise.

Secondly and related to the above, financial institutions should provide frequent cyber-security related training to staff and employees. This should be frequent and incremental to enable staff and employees to be up-to-date and well informed on the vast cyber-security threats that face the banking sector. Professionals and cyber-security experts such as information security officers, forensic investigation officers and software developers should be involved in such trainings. This will ensure the best minds in the cyber-security scene are involved.

This study takes note of the importance of creating cyber-security awareness among the banking service consumers. The financial institutions and the sector associations together with the help of sector regulatory institutions and policy makers should focus on increasing public awareness on cyber-security practices. Programs and such activities should also focus on emerging innovations within the banking sector such as the recent emergence of agency banking, internet banking, and mobile banking and other innovative financial products that the banking sector launch.

Financial institutions should strengthen their efforts directed towards meeting of the banking sector cyber-security regulations and protection frameworks. As revealed in the study, financial institutions are notorious and at times circumvent or ignore the cyber-security regulation requirements. Regulations for instance, linking of OTP to phone IMEI number and client account number is a feature for verification of transactions and client identity. This has not been effectively observed by all financial institutions which target profits as an end game.

Concentration on profit and market share in the highly competitive banking sector has therefore, led to lax implementation of standardized regulations. This should therefore be addressed through observing all regulatory requirements within the sector.

Another important revelation in this study is that Third parties pose a risk to the cyber-security of financial agencies. A Third party risk assessment is therefore important as should be made a requirement through a Third party regulatory framework. Through this, Third parties such as those who provide banking networks, systems, firewalls and softwares will be vetted and assessed for any risks before procurement and installation of such systems. The current trends of system integration where firewalls are connected to operating systems which are also interlinked with banking systems may be fatal if any backchannels are available for exploitation. Therefore, Third parties should be constantly monitored to ensure remote connections do not exist. Defence depths can be met when banks also vet all the Third party vendors and ensure only the approved and reliable vendors are certified for supply of infrastructure.

Also related to the above is the modern system integration caused by banking service innovations. This system integration, for example linking mobile money to ATMs is a complex system interdependence that may introduce cyber security risks. Such innovations, meant to achieve functionality and efficiency need to be constantly assessed and monitored. Therefore, system integration testing and monitoring should be part of the standard operating procedures to ensure such innovations are safe and pose no risks to the client transactions.

4.3.2 Recommendations for Regulatory Institutions and Banking Sector Associations

The regulatory institutions and sector associations should strengthen regulatory and enforcement capabilities in the cyber-security scene. Regulations requiring strong cyber-security measures in financial institutions need to be introduced and all outdated ones need to be revised. This is in line with the quick evolving cyber-crime terrain as criminals keep inventing new methods and systems of exploitation. Initiatives and efforts also need to concentrate on enhancement of the capacities of law enforcement to increase investigation, prosecution and punishment for cyber criminals. Further to this, the CBK should renew its efforts and enforce regulations in a stringent manner as banks have been found to blatantly flout sector regulations.

Regulatory institutions such as the CA, CBK and banking sector association the Kenya Bankers Association (KBA) should bring together the banks and introduce certification for Third party vendors in the banking sector. Together these institutions, the financial institutions should share information and harmonize vendors in the sector. This study notes that the multiplicity of Third party vendors used by financial institutions has brought about the need for regulation. This will protect financial institutions from unscrupulous/suspicious vendors who lack strong internal security systems and are susceptible to exploitation by criminals.

This study recommends that it is important for sector regulatory institutions to adopt and enforce international best practices and standards. International standards such as ISO 27001, GDPR, and NIST should be made mandatory for financial institutions in the country. The ISO 27001 is a certification standard meant to manage information security in a holistic way. It integrates the technological and non-technological controls in financial institutions. The National Institution of Standards and Technology (NIST) is a cyber-security framework that provides guidelines for mitigating a financial institution's cyber-security risks. Lastly, General Data Protection Regulation (GDPR) is another standard applied in the European Union and regulates personal data of clients of an institution. These standards which are international in nature should all be adopted domestically to govern the banking sector.

4.3.3. Recommendation to the Government of Kenya

This study notes that cyber-security and cybercrime is addressed through a disintegrated approach where various institutions in government and also the private sector address cyber-crime independently. This study therefore, recommends that the Government of Kenya should form a dedicated national agency to address cybercrime. This agency should take the form of a multi-sectoral agency with officers seconded from relevant government Ministries, Departments and Agencies (DCI, Min. ICT, Min. Finance, CA, CBK, ODPP, KBA, judiciary etc.) for purposes of addressing its needs. In addition, this agency should closely work with the private sector players and other stakeholders to address cyber-crime which has become a universal challenge to both public institutions and the private sector across the country. This agency should be further embedded in Kenya's legal framework and equipped with necessary resources to enable it to effectively discharge its mandate.

4.4 Suggestions for Future Research

This study has proven that cyber-crime is an existential threat to the banking sector. We hereby suggest that future research should focus on investigating the national security threats posed by proceeds of cyber-crime from Kenya's financial institutions.

References

- Adelmann, F., Elliott, M. J. A., Ergen, I., Gaidosch, T., Jenkinson, N., Khiaonarong, M. T., & Wilson, C. (2020). *Cyber risk and financial stability: It's a small world after all*. International Monetary Fund.
- Agrawal, S. (2016). Cyber Crime in Banking Sector. *The Origin of Knowledge. Volume 3*. 1-19
- Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., & Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy* (pp. 265-300). Springer, Berlin, Heidelberg.
- Ayuo, T. (2021). Kenya: Why Cybercrimes Are Also Crimes Against Humanity. Retrieved on 10th September 2021 from <https://allafrica.com/stories/202107290831.html>
- Bouveret, A. (2018). *Cyber risk for the financial sector: A framework for quantitative assessment*. International Monetary Fund.
- Brenner, S. W. (2010). *Cybercrime: criminal threats from cyberspace*. ABC-CLIO.
- Broadhurst, R. (2006). "Developments in the global law enforcement of cyber-crime", Policing: An International Journal of Police Strategies & Management, Vol. 29 Issue: 3, pp.408-433
- Business Daily (February, 2021). Cyber-attacks in Kenya up by half to hit 56m in three months. Retrieved on 12th July, 2021 from <https://www.businessdailyafrica.com/bd/corporate/companies/cyber-attacks-in-kenya-56m-in-three-months-3285438>
- Calderoni, F. (2010). The European legal framework on cybercrime: striving for an effective implementation. *Crime, law and social change*, 54(5), 339-357.
- Camillo, M. (2017). Cybersecurity: Risks and management of risks for global banks and financial institutions. *Journal of Risk Management in Financial Institutions*, 10(2), 196-200.
- Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). The economic impact of cyber-attacks. *Congressional Research Service Documents, CRS RL32331 (Washington DC)*.
- Castells, M. (2002). *The Internet galaxy: Reflections on the Internet, business, and society*. Oxford University Press on Demand.
- Central Bank of Kenya (2015). Bank Supervision Annual Report 2015. Government Printers
- Central Bank of Kenya (2020). Bank Supervision Annual Report 2020. Government Printers
- Chevers, D. A. (2019). The impact of cybercrime on e-banking: A proposed model. In *CONF-IRM* (p. 11).

- Chevers, D. A. (2019). The impact of cybercrime on e-banking: A proposed model. In *CONF-IRM* (p. 11).
- Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management*, 23(1), 1-11.
- Clarke, R. V., & Felson, M. (2017). Introduction: Criminology, routine activity, and rational choice. In *Routine activity and rational choice* (pp. 1-14). Routledge.
- Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, 588-608.
- Cohen, L. E., & Felson, M. (2010). Social change and crime rate trends: A routine activity approach (1979). In *Classics in environmental criminology* (pp. 203-232). Routledge.
- Communications Authority (2017). Annual Report 2016-2017. Retrieved on 12th September, 2021 from <https://ca.go.ke/wp-content/uploads/2018/04/Annual-Report-for-the-Financial-Year-2016-2017.pdf>
- Communications Authority (2021). First Quarter Sector Statistics Report for the Financial Year 2021/2022 (JULY - SEPTEMBER 2021). Retrieved on 12th September, 2021 from <https://www.ca.go.ke/wp-content/uploads/2021/12/Sector-Statistics-Report-Q1-2021-2022.pdf>
- Gumbi, D. (2018). *Understanding the threat of cybercrime: A comparative study of cybercrime and the ICT legislative frameworks of South Africa, Kenya, India, the United States and the United Kingdom* (Master's thesis, University of Cape Town).
- Hutchings, A., & Hayes, H. (2009). Routine activity theory and phishing victimisation: who gets caught in the 'net'?. *Current Issues in Criminal Justice*, 20(3), 433-452.
- Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Cybercrime classification and characteristics. In *Cyber Crime and Cyber Terrorism Investigator's Handbook* (pp. 149-164). Syngress.
- Kenneth J. Knapp & William R. Boulton (2006) Cyber-Warfare Threatens Corporations: Expansion into Commercial Environments, *Information Systems Management*, 23:2, 76-87
- Kenyan Magazine (2021). List Of Best Cyber Security Companies in Kenya retrieved from <https://kenyanmagazine.co.ke/top-10-best-cyber-security-companies-in-kenya/>
- Kigen, P. M., Kisutsa, C., Muchai, C., Kimani, K., Shiyayo, B., & Mwangi, M. (2014). *Kenya Cyber Security Report 2014*. Tespok.
- Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, 22(2), 77-81.

- Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber-crime on the financial sector. *Computers & Security*, 45, 58-74.
- Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research*, 23(3), 287-300.
- Liao, R., Balasinorwala, S., & Rao, H. R. (2017). Computer assisted frauds: An examination of offender and offense characteristics in relation to arrests. *Information Systems Frontiers*, 19(3), 443-455.
- Lockheed Martin Corporation (2015). Combatting the Biggest Cyber Threats to the Financial Services Industry. Retrieved from https://www.ciosummits.com/Financial_Services_Cyber_Challenges_White_Paper.pdf
- Maurer, T., & Nelson, A. (2021). The global cyber threat. *Finance & Development*, 24-27.
- Mester, L. J. (2019). Cybersecurity and financial stability. Retrieved from <https://www.clevelandfed.org/newsroom-and-events/speeches/sp-20191121-cybersecurity-and-financial-stability>
- Moitra, S. D. (2005). Developing policies for cybercrime. *European Journal of Crime Criminal Law and Criminal Justice*, 13(3), 435.
- Mugari, I., Gona, S., Maunga, M., & Chiyambiro, R. (2016). Cybercrime-the emerging threat to the financial services sector in Zimbabwe. *Mediterranean Journal of Social Sciences*, 7(3 S1), 135.
- Munyori, M. and Mumbi, J. (2020). The Rise of Cyber Crimes in Kenya: How Effective are Our Laws? Retrieved on 23 November 2022 from serianu.com/contact.html
- Nachmias, C., & Nachmias, D. (2007). *Study guide for research methods in the social sciences*. Macmillan.
- OECD (2007). Malicious Software: A security threat to the internet economy. Ministerial background report DSTI/ICCP/REG(2007)5/FINAL.
- Pettersson, M. (2012). Banks likely to remain top cybercrime targets. Symantec Corporation.
- Quarshie, H. O., & Martin-Odoom, A. (2012). Fighting cybercrime in Africa. *Computer Science and Engineering*, 2(6), 98-100.
- Raghavan, A. R., & Parthiban, L. (2014). The effect of cybercrime on a Bank's finances. *International Journal of Current Research & Academic Review*, 2(2), 173-178.
- Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D. M., & Moore, A. P. (2005). Insider threat study: Illicit cyber activity in the banking and finance sector.

- SERIANU (2018). Africa Cyber Security Report – Kenya. Retrieved on 23 November 2022 from <https://www.serianu.com/downloads/KenyaCyberSecurityReport2018.pdf>
- Staal, F. J. (2015). *Cybercrime and the impact on banks' frontline service employees: a qualitative study towards the impact of cybercrime on the experiences, concerns and actions taken by Frontline Service Employees within the banking sector* (Master's thesis, University of Twente).
- Steinmetz, K. F., & Yar, M. (2019). Cybercrime and society. *Cybercrime and Society*, 1-368.
- Taherdoost, H. (2016). Sampling methods in research methodology; how to choose a sampling technique for research. *How to Choose a Sampling Technique for Research (April 10, 2016)*.
- Tariq, N. (2018). Impact of cyberattacks on financial institutions. *Journal of Internet Banking and Commerce*, 23(2), 1-11.
- Vijayalakshmi, P. Priyadarshini, V. and Umamaheswari, K. (2021). Impacts of Cyber Crime on Internet Banking. *International Journal of Engineering Technology and Management Sciences*. Issue: 2 Volume No.5 March – 2021
- Wall, D. (2007). *Cybercrime: The transformation of crime in the information age* (Vol. 4). Polity.
- Wall, D. S. (2015). Dis-organised crime: Towards a distributed model of the organization of cybercrime. *The European Review of Organised Crime*, 2(2).
- Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. *International Journal of Law, Crime and Justice*, 62, 100415.
- Wasuna (2021). East Africa: How Rwanda Stopped Kenyan Cyber gang. Retrieved on 1st September, 2021 from <https://allafrica.com/stories/202107250051.html>
- Yin, R., 2009. *Case study research: Design and methods* (4th ed.). Los Angeles: Sage

Appendices

Appendix I: Questionnaire

Section A: Demographic Information

1. Gender

Male Female

2. Age Bracket

≤25 Years
26-35 Years
36-45 Years
46-55 Years
56+ Years

3. Level of Education

Post-Graduate
Graduate
College Dip.
Secondary
Others

4. Type of Bank

Domestic owned banks
Foreign owned bank
Microfinance banks

Section B: Financial Impacts of Cybercrime on Kenya's Banking Sector

5. Which are the most common types of Cybercrime in Kenya's banking sector? (*You may tick more than one*)

Hacking
Identity theft
Electronic card fraud
Malware
Phishing

- Card information skimming
- Mobile Banking Breaches

6. Cybercrime has a financial cost on Kenya's banking sector.

- Strongly Agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly Disagree

7. What is the estimated annual financial loss incurred by your bank as a result of cybercrime? (KES)

8. Countering cybercrime activities in the banking sector has a high cost to Kenya's economy

- Strongly Agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly Disagree
- No extent

9. To what extent does cybercrime impact on the economy's ability to attract foreign direct investment?

- Very great extent
- Great extent
- Moderate extent
- Little extent
- No extent

Section B: Impacts of Cybercrime on Bank Data in Kenya's Banking Sector

10. Which are some of the common types of data targeted cyberattacks in Kenya's banking sector? (*You may tick more than one*)

- Ransomware
- Malware
- Phishing
- Denial of Service

11. What are the major types of bank data losses as a result of cyber-attacks on banks in Kenya? (*You may tick more than one*)

- Client information loss
- Data stealing
- Customer frustration
- Destruction of PR

12. To what extent does data loss from cyber-attacks negatively impact Kenya's banking sector?

- Very great extent
- Great extent
- Moderate extent
- Little extent
- No extent

Section C: Cyber security measures put in place in Kenya's Banking Sector

13. What cyber security measures have been put in place by your bank to prevent cyber-attacks?

14. Which methods are used to prevent cyber-attacks in Kenya's banking sector? (*Tick more than one*)

- Tight internal security
- Cyber security assessment
- Cyber security training
- Cyber security audit

15. To what extent do existing cyber security measures prevent cyber-attacks in Kenya's banking sector?

- Very great extent
- Great extent
- Moderate extent
- Little extent
- No extent

16. To what extent do cybercriminals by-pass existing security measures Kenya's banking sector?

- Very great extent
- Great extent
- Moderate extent
- Little extent
- No extent

Section D: Challenges Facing Cyber security measures put in place by Kenya's Banking Sector

17. How satisfied are you with regulatory institutions ability to implement cybercrime prevention measures in the banking sector?

- Very dissatisfied
- Dissatisfied
- Neither satisfied nor dissatisfied
- Satisfied
- Very satisfied

18. To what extent do state legal frameworks cover cybercrime related issues in the banking sector?

- Very great extent
- Great extent
- Moderate extent
- Little extent
- No extent

19. How effective are the current cyber security legal frameworks in prosecuting and convicting cybercriminals

- Very effective
- Effective
- Moderately effective
- Less effective
- Not effective

20. How effective are the sector cyber security measures put in place to fight cybercrime?

- Very effective
- Effective
- Moderately effective
- Less effective
- Not effective

21. How effective are the regional cooperation mechanisms in the fight against cyber terrorism in the East Africa region?

- Very effective
- Effective
- Moderately effective
- Less effective
- Not effective

22. Is there any other issue of interest in matters of cyber-crime in the financial sector that you would like to add? _____

Appendix II: Interview Guide

1. Which are the most common types of Cybercrime in Kenya's banking sector?
2. What are some of the economic costs of cyber-crime to the banking sector
3. How can you describe the costs associated with countering cybercrime in the banking sector
4. What is the estimated financial loss from cyber-attacks on Kenya's banks
5. How do cyber-attacks targeting bank data impact the banking sector?
6. How have online and mobile banking platforms affected the cyber-criminal activities in the banking sector
7. What are the main cyber security measures for preventing cyber-attacks in the banking sector?
8. What are some of the measures implemented by regulatory institutions to prevent cyber-crimes in the banking sector
9. How robust have legal frameworks covered cyber-crime related issues in the banking sector
10. In your opinion, are the current cyber security legal frameworks for prosecuting and convicting cybercriminals robust? Kindly explain
11. In your opinion, how would you describe the effectiveness of the cooperation mechanism in the fight against cyber-crime in the East Africa region?

Appendix III: Consent Letter

The purpose of this study is to find out the *Impact of Cybercrime on the Finance Sector: A Case of Banks in Nairobi County, Kenya (2008 - 2022)*. Participants are required to respond to the researcher through an interview session where questions on cybercrime and cyber security will be asked. The researcher will take notes and at times statements will be accurately written for use in analysis. Although we feel there will be no harm or intrusion from this research, we hereby take note that participants are protected and in the event they feel uncomfortable to respond, they can choose to skip or terminate the interview. Participation in this study is voluntary. The data being collected will be treated with the utmost confidentiality, respondents' identity will be treated anonymously and all the information will be safely stored.

I have received the introduction letter of the researcher from the University of Nairobi. I have read and understood the objectives of the study. Information on this research has been provided to me and I have accepted to participate. My participation is purely voluntary.

If you agree to participate, kindly sign in the area provided below.

Organisation/Institution: _____

Name: _____

Signature: _____

Date: _____

Appendix IV: Introduction Letter



University of Nairobi
FACULTY OF ARTS AND SOCIAL SCIENCES
Department of Political Science & Public Administration

Telegrams: "Varsity", Nairobi
Telephone: 318262 ext. 28171
Telex: 22095 Varsity
Email: dept-pspa@uonbi.ac.ke

P.O. Box 30197
Nairobi, Kenya

10/9/2022

=====

TO WHOM IT MAY CONCERN

=====

AUTHORIZATION TO CONDUCT FIELD RESEARCH

=====

This is to confirm that Ibrahimnur Abdi Adan of Registration Number (C50/5205/2017) is a bonafide student in the Department of Political Science and Public Administration, University of Nairobi.

Ibrahimnur is pursuing a Degree of Master of Arts in Strategic and Security Studies. He is researching on, **"Impact of Cyber Crime on Financial Institutions: Case Study of Banks in Nairobi"**.

He has successfully completed the first part of his studies (Course Work) and is hereby authorized to proceed to conduct Field Research. This shall enable the student to collect relevant data for his academic work.

It is against this background that the Department of Political Science and Public Administration, University of Nairobi requests your assistance in enabling the student to collect relevant academic data. The information obtained shall be used specifically and only for academic purpose.

The student is expected to abide by your regulations and the ethics that this exercise demands. In case of any clarification, please feel free to contact the undersigned.

Thank you.



Professor Fred Jonyo (PhD, Makerere)
Chairman,
Department of Political Science and Public Administration,
UNIVERSITY OF NAIROBI

Appendix V: NACOSTI Permit



REPUBLIC OF KENYA



**NATIONAL COMMISSION FOR
SCIENCE, TECHNOLOGY & INNOVATION**

Ref No: 998951

Date of Issue: 21/November/2022

RESEARCH LICENSE



This is to Certify that Mr.. IBRAHIMNUR ABDI ADAN of University of Nairobi, has been licensed to conduct research as per the provision of the Science, Technology and Innovation Act, 2013 (Rev.2014) in Nairobi on the topic: IMPACT OF CYBERCRIME ON THE FINANCE SECTOR: A CASE OF BANKS IN NAIROBI COUNTY, KENYA (2008 - 2021) for the period ending : 21/November/2023.

License No: NACOSTI/P/22/22058

998951

Applicant Identification Number

Director General

**NATIONAL COMMISSION FOR
SCIENCE, TECHNOLOGY &
INNOVATION**

Verification QR Code



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

See overleaf for conditions

Appendix VI: Cyber Security Companies

1. East Africa Recovery Experts Contacts Details: 0716079961
2. Cyber Security Africa Contacts Details: 0722 102 854 info@cybersecurityafrica.com
3. Serianu Limited +254 702 847 570, +254 (0) 718 181 800 info@serianu.com
4. Inceptor Kenya +254 728 456 781, +254 712 369 902, admin@inceptor.co.ke
5. White Leaf Group (254) 724810865 info@whiteleaf.co.ke
6. Techinnovar Limited 0771 599172 info@techinnovar.com
7. Central Information System International (CISI)
8. Enovise Cyber Security Company +254 727 950 013 or 0714 370 253 info@enovise.com
9. Protec. Contacts Details: 020 2722485
10. Crystal technologies Limited

Appendix VII: Micro-finance Banks in Nairobi County

1. Kenya Women Microfinance Bank Limited
2. Faulu Microfinance Bank Limited
3. Rafiki Microfinance Bank Limited
4. SMEP Microfinance Bank Limited
5. Sumac Microfinance Bank Limited
6. KEY Microfinance Bank Limited
7. Maisha Microfinance Bank Ltd
8. Caritas Microfinance Bank Limited
9. Century Microfinance Bank Limited
10. U & I Microfinance Bank Limited
11. Uwezo Microfinance Bank Limited
12. Choice Microfinance Bank Limited
13. Daraja Microfinance Bank Limited
14. Muungano Microfinance Bank Limited

Appendix VIII: Commercial Banks in Nairobi County

1. NCBA Bank Kenya Ltd.
2. Equity Bank Kenya Ltd
3. KCB Bank Kenya Ltd
4. Co-operative Bank of Kenya Ltd
5. ABSA Kenya Plc
6. Diamond Trust Bank (K) Ltd
7. Stanbic Bank Kenya Ltd
8. Standard Chartered Bank (K) Ltd
9. Family Bank Ltd
10. National Bank of Kenya Ltd
11. HFC Limited
12. Ecobank Kenya Ltd
13. I & M Bank Ltd.
14. Bank of Africa Kenya Ltd
15. Bank of Baroda Ltd
16. Prime Bank Ltd
17. Bank of India
18. Citibank N.A. Kenya
19. Sidian Bank Limited
20. SBM Bank (Kenya) Ltd.
21. Kingdom Bank Limited
22. Access Bank (Kenya) PLC
23. Gulf African Bank Ltd
24. First Community Bank Ltd
25. Consolidated Bank of Kenya Ltd
26. Credit Bank Ltd
27. African Banking Corporation Ltd
28. Spire Bank Limited
29. Guaranty Trust Bank (Kenya) Ltd
30. Guardian Bank Limited
31. Paramount Bank Ltd
32. UBA Bank Kenya Ltd
33. M-Oriental Commercial Bank Ltd
34. DIB Bank Kenya Ltd
35. Habib Bank A.G. Zurich
36. Middle East Bank Ltd
37. Victoria Commercial Bank Ltd
38. Mayfair CIB Bank Ltd

39. Development Bank of Kenya Ltd