

UNIVERSITY OF NAIROBI

DEPARTMENT OF SOCIOLOGY

**ASSESSING THE CAPACITY OF CID HEADQUARTERS CYBER CRIME
PREVENTION UNIT FOR THE PREVENTION OF CYBER BASED
FINANCIAL CRIME IN KENYA**

**A RESEARCH PROJECT IN FULFILMENT OF THE REQUIREMENTS FOR
THE AWARD OF A MASTERS DEGREE IN SOCIOLOGY (CRIMINOLOGY)**

NAME: OKWARA N. ISAAC

REG NO: C50/ 70967 /09

SUBMITTED TO: DR BENSON AGAYA

NOVEMBER, 2011

University of NAIROBI Library

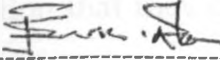


0472162 7

DECLARATION

DECLARATION BY CANDIDATE

I, hereby declare that this Research Project is my original work and has not been submitted for examination in any other University.

Signed-----

Date-----21/10/2011

Isaac Nyongesa Okwara


Reg. No. C50/70967/2009

UNIVERSITY OF NAIROBI

DEPARTMENT OF SOCIOLOGY AND SOCIAL WORK

DECLARATION BY SUPERVISOR

This Project has been submitted for examination with my approval as the University Supervisor.

Signed-----

Date-----21/10/2011

Dr. Benson Agaya

UNIVERSITY OF NAIROBI

DEPARTMENT OF SOCIOLOGY AND SOCIAL WORK

DEDICATION

First and foremost, I wish to dedicate this work to God Almighty for giving me the strength and resources to complete this self-sponsored programme. To my parents Virginia and Joseph the late who sacrificed a lot to ensure that I received the best education that they could afford. May God bless you abundantly with more knowledge. To my caring wife Leanne, Sons Albright and Rahm for their prayers and word of encouragement.

I also wish to dedicate this work to my siblings, for constant encouragement and advice, which ensured that I did not lose focus throughout the duration of the programme. Their words of encouragement kept me going even when the challenges seemed too hard to overcome. To my benefactors Fr.Peter Meienberg(OSB),The late Fr.Benard Bennbeck(MHM),Fr.Louis Van der Werf(MHM),Fr.Sean O'Connor(SJ) for their spiritual and financial support. Finally, I wish to dedicate this work to my classmates for being such good companions throughout this long and intellectually stimulating journey.

ACKNOWLEDGEMENTS

I wish to express my sincere thanks to my supervisor Dr. Agaya for his advice, patience and tireless efforts without which I would not have completed this project. I would also want to thank the Department of Sociology lecturers for their support and dedication. My entire family for giving me moral support in the course of my studies.

Thank you all and may God bless you abundantly.

TABLE OF CONTENTS

DECLARATION	ii
DEDICATION	iii
ACKNOWLEDGEMENTS	iv
TABLE OF CONTENTS	v
LIST OF FIGURES.....	ix
LIST OF TABLES.....	ix
ABBREVIATIONS.....	xi
ABSTRACT	x
CHAPTER ONE	1
INTRODUCTION	1
1.1 Background.....	1
1.2 Problem Statement.....	7
1.3 Objectives of the study	10
1.3.1 General Objective.....	10
1.3.2 Specific Objectives	10
1.4 Rationale.....	10
1.5 Scope and Limitations	11
CHAPTER TWO.....	12
LITERATURE REVIEW.....	12
2.1 Introduction.....	12
2.1.1 The Role of the Internet.....	12
2.1.2 Information Security.....	15
2.2 Trends in Cyber Crime.....	16
2.2.1 Trends Globally	16
2.2.2 Trends in Kenya	19
2.2.3 The Kenya Banking Sector.....	20
2.2.4 Legislation on Cyber Crime	21

2.3 Structures and Mechanisms to Prevent Cyber Crime in Financial Institutions	23
2.3.1 Legal Framework	23
2.3.2 Human Resources	25
2.3.3 Technical Resources	27
2.4 Obstacles to Prevention of Cyber Crime	31
2.5 Theoretical Framework	35
2.5.1 Control Theory	36
2.5.2 Rational Choice Theory	37
2.5.3 Social Systems Theory	38
2.6 Conceptual Framework	39
CHAPTER THREE	42
RESEARCH METHODOLOGY	42
3.1 Research Site	42
3.2 Research Design	42
3.4 Sampling Design	43
3.5 Tools and Techniques of Data Collection	44
3.6 Data Analysis	44
CHAPTER FOUR	46
DATA ANALYSIS, INTERPRETATION AND PRESENTATION	46
4.1 Introduction	46
4.2 Background information	46
4.2.1 Distribution of Respondents	46
4.2.2 Gender of Respondents	47
4.2.3 Age of Respondents	47
4.2.4 Designation of Respondents	48
4.2.5 Respondent's Length of Service in the Police Force	49
4.2.6 Respondent's Length of Service in CID CCU	51
4.2.7 Respondent's Highest Educational Attainment	51

4.2.8 Respondent's Criteria for Recruitment	52
4.3.1 Cases of financial crime investigated.....	53
4.3.2 Number of cases that occurred in the past one year.....	54
4.3.3 Number of Cases handled in the past six months	55
4.3.4 Number of cases handled in the past three months	56
4.3.5 Types of cases of financial based cyber crime solved.....	57
4.3.6: Types of cases of financial based crime not solved.....	58
4.4 Findings and Analysis on Objective 2: Structures and Mechanisms for Cyber Policing and Crime Prevention in Financial Institutions in Kenya	59
4.4.1 Respondent's Training prior to posting to CCU	59
4.4.2 Training after posting to CCU	60
4.4.3 Responsibilities assigned in current post	61
4.4.4 Mechanisms for cyber crime prevention in financial institutions	61
4.5.1: Reasons for not solving cases.....	63
4.5.2: Liaisons established to support work	64
4.5.3: Liaisons not established but important to support work.....	65
4.5.4: How deployment practices support work	66
4.5.5: How deployment practices do not support work.....	67
4.6 Findings and Analysis on Objective 4: Capacity of CID CCU in preventing Cyber based Financial Crimes in Kenya.....	69
4.6.1 Ways of addressing limitations in operations	69
4.6.2 Resources required by Respondents to function effectively in the unit	70
4.6.3 Adequately supplied resources	71
4.6.4 Resources that are not adequately supplied	72
4.6.5 Causes of deficiency in supply of resources	72
4.6.6 Action to ensure own preparedness for the role	73
CHAPTER FIVE	75
SUMMARY OF FINDINGS, CONCLUSION AND RECOMMENDATIONS.	75
5.1 Introduction.....	75

5.2 Summary of Findings.....	75
5.3 Conclusion	77
5.4 Recommendations	78
5.4.1 Policy Recommendations	78
5.4.2 Recommendations for Further Research	79
REFERENCES.....	80
APPENDIX I	88
INTRODUCTION LETTER.....	88
APPENDIX II.....	89
RESEARCH QUESTIONNAIRE FOR DETECTIVES AT CID CCU.	89
APPENDIX III	92
KEY INFORMANT INTERVIEW GUIDE FOR OFFICIALS FROM CCK, COMPUTER SOCIETY OF KENYA, THE JUDICIARY AND A BANK.	92

LIST OF FIGURES

Figure 1: Capacity of CID CCU for Prevention of Cyber Based Financial Crimes	40
Figure 2: Respondent's Sex.....	47
Figure 3: Respondent's Age Category	48
Figure 4: Respondent's Designation	49
Figure 5: Respondents' Length of Service in the Police Force.....	50
Figure 6: Respondents' Length of Service in the CID CCU	51
Figure 7: Distribution of respondents according to highest educational attainment	52

LIST OF TABLES

Table 1: Distribution of respondents according to criteria for recruitment to ccu	52
Table 2: Cases of Financial Crime investigated by Respondents since Posting.....	54
Table 3: Respondents' recollection of the number of cases handled in the past one year.....	55
Table 4: Number of cases that occurred in the past six months.....	56
Table 5: Number of cases that handled in the past three months.....	57
Table 6: Financial based crime cases solved	58
Table 7: Financial based crime cases not solved.....	58
Table 8: Training prior to posting to CCU	59
Table 9: Training after posting to CCU.....	60
Table 10: Responsibilities assigned in current post	61
Table 11: Mechanisms for cyber crime prevention in financial institutions	62
Table 12: Respondents' reasons for not solving cases	64
Table 13: Awareness of the liaisons established to support work.....	65
Table 14: Respondents' views on the liaisons not established but important to support work	66

Table 15: Respondents' views on how deployment practices support work.....	67
Table 16: Respondents' views on how deployment practices do not support work	68
Table 17: Respondents' suggestions on addressing limitations in operations	70
Table 18: Resources required to function effectively in the position	71
Table 19: Respondents' views on resources that are adequately supplied	72
Table 20: Resources that are not adequately supplied	72
Table 21: Causes of deficiency in supply of resources	73
Table 22: Respondent's action to ensure own preparedness for the role.....	74

ABBREVIATIONS

ACFE	-	Association of Certified Fraud Examiners
AML	-	Anti- Money Laundering
ARPANET	-	Advanced Projects Research Agency Network
ATM	-	Automated Teller Machine
BFID	-	Banking Fraud Investigation Department
CBK	-	Central Bank of Kenya
CCK	-	Communications Commission of Kenya
CCU	-	Cyber Crime Unit
CID	-	Criminal Investigation Department
EFT	-	Electronic Fund Transfer
ICT	-	Information Communication Technology
IT	-	Information Technology
KBA	-	Kenya Bankers Association
KEPSS	-	Kenya Electronic Payments and Settlement System.
OECD	-	Organization for Economic Development
POS	-	Point of Sale
PwC	-	PricewaterhouseCoopers
RTGS	-	Real Time Gross Settlement
SWIFT	-	Society for World Wide Interbank Financial Communication
UNODC	-	United Nations Office for Drugs and Crime

ABSTRACT

The use of cyber space as a platform and catalyst for sophisticated as well as organized crimes is of concern to governments worldwide. Cyber crime is currently a major global concern given the economic losses companies incur world wide as a result of the crime. This study sought to assess the capacity of CID Headquarters Cyber Crime Prevention Unit in preventing cyber based financial crimes in Kenya. Unofficial reports show that in the third quarter of the year 2010, bank fraud tripled to Kshs 1.7 billion.

The site of the study was CID Headquarters Cyber Crime Unit and involved 32 CCU officers while additional information was sought from 12 key informants who included 4 bank officials, a CCK official, an official of the Computer Society of Kenya, 4 specialists from the computer forensic firms an officer from the Anti Terrorist Police Unit. The study revealed that a majority of the respondents (40.6 percent) indicated that all resources were not adequately supplied at the unit while 31.3 percent of the respondents said that transport and forensic tools were not adequately supplied.

The study found out that out of all the respondents, 15.6 percent of the said that qualified personnel were in short supply in the unit while only 12.5 percent identified training as not provided at the unit. It was also found that majority of the respondents (37.5 percent) attributed lack of resources at CID CCU to an inadequate budget while 31.3 percent laid the blame on low understanding of cyber crime and poor ICT policy. Majority of the respondents (40.6 percent) indicated that liaisons and intelligence sharing was key in cyber crime prevention while 28.1 percent proposed upgraded IT infrastructure. Enhanced legislation was cited by 18.8 percent of the respondents while training of stakeholders was indicated by 12.5 percent of the respondents.

The study also revealed that majority (43.8 percent) of the officers at CID CCU investigated either between 1- 15 cases or between 53-200 cases of financial based cyber crime in the past one year. Only 12.5 percent of the officers investigated between 15 and 52 cases of financial based cyber crime in the past one year. The most cited reason given by 53.1 percent of the officers for not being able to solve cases of financial based cyber crime was the lack of transboundary cooperation followed by legal and investigations drawbacks which was chosen by 34.4 percent of the officers. Lack of cooperation by ISPs was selected by 6.3 percent of the respondents while political interference and lack of software equipment were each chosen by 3.1 percent of the officers.

It was also found that most of the officers (28.1 percent) were for chose continuous and contextualized training as the best way of addressing limitations in operations at the CID CCU. Enhancing funding for equipment, software and remuneration was cited by 21.9 percent of the officers while placement of qualified management was the choice of 15.6 percent of the officers. 12.5 percent of the officers were for recruiting and retaining qualified officers whereas the same percentage cited enhancing legislation and policy making. 9.4% of the officers were for correct placement and specialization.

The study therefore concludes that high turnover of specialized officers at the CCU unit was as a result of transfers within the force or resignations. Inadequate budgetary allocations and resources, lack of recognition and liaisons with financial institutions and other stakeholders and also the lack of mutual legal agreement and clear legislation have greatly accounted for the incapacitation of CID CCU in the prevention of financial based cyber crime in Kenya.

Important recommendations offered in this study include government to ensure that the legal instruments available are reviewed constantly to ensure that they

are punitive and deterrent in nature. The government should sensitize and educate law enforcement agencies, the public, and financial institutions on the importance of protection against cyber based financial crime. Organizations such as the KBA should collaborate with industry players and stakeholders to offer sensitization programs. The government should ensure strong legislation and legal cooperation with other countries. Capacity of CID CCU should be increased through adequate budgetary allocations, proper deployment practices and stronger liaisons especially with financial institutions and other intergovernmental agencies such as Immigration, Kenya revenue authority, and treasury.

CHAPTER ONE

INTRODUCTION

1.1 Background

Cyber crime exists within and has its origins in the Internet which according to Grant and Meadows (2002) is a worldwide connection of computer networks that allows a user to access information located anywhere else on the network. Grant and Meadows (2002) further explain that the Internet was created in the 1950s when the United States Department of Defense sought ways to form a decentralized communications system that would allow researchers and government officials to communicate with one another in the aftermath of a nuclear attack from the Russia.

A computer network seemed to be the most logical way to accomplish this hence the military formed the Advanced Projects Research Agency (ARPA) to study ways to connect networks and the result was the Internet. ARPANET used Transmission Control Protocol/Internet Protocol (TCP/IP) which is a method of data transmission in which information is broken into 'packets' that are sent to a given destination and upon arrival are re-assembled to create the original message. The network grew as more computers joined it to form the World Wide Web (www) which was invented by Tim Bernes-Lee, a researcher at the European Organization for Nuclear Research. He also devised a computer language called Hypertext Markup Language (HTML) which allows users to explore information on the internet (Grant and Meadows, 2002).

Cyber crime is the use of a computer as an instrument to further illegal ends such as committing fraud, dealing in child pornography and intellectual property rights infringements, making illegal gains from others and stealing identities or violating privacy (Encyclopedia Britannica online). Granville (2003) defines cyber crime as unauthorized access to or the illicit tampering with files and data in

computer networks through unauthorized copying, modification or destruction. It is also computer network sabotage through viruses, worms, Trojan horses and denial of service attacks or the use of information systems to commit or advance traditional crimes like fraud, forgery, money laundering as well as acts of terrorism. It is also computer mediated espionage or violation of privacy in the acquisition or use of personal data and also the theft or damage of computer hardware.

The above definitions indicate that cyber crime is a criminal activity performed using computers and the internet. The computer may be used as a tool or as a target. It may be used as a tool to commit financial crimes or as a target for unlawful acts such as unauthorized access to computer systems or networks and physical theft or damage of the computer.

Apart from communication, the Internet is also used for commerce and involves trade in goods or services over the Internet or e-commerce. According to Forester Research, the global internet economy reached USD 6.9 trillion in 2004 when e-commerce accounted for 8.6 % of world wide sales of goods and services (Dutta and Roy, 2008). This rapid-growth in internet based commerce has seen a concomitant rise in cyber crime. The networked environment enables criminals to exploit the borderless marketplace by setting up false websites to trick customers into divulging their credit card numbers and subsequently getting money out of their accounts. In some cases, criminals have been able to access client records on internet banking or e-banking then making fraudulent transactions resulting to loss of money from the accounts.

Cyber crime is currently a major global concern given the economic losses companies incur world wide as a result of the crime. The PricewaterhouseCoopers Global Crime Survey for 2009 estimated that out of

1000 companies in 50 countries, a total of almost USD 0.8 million was lost in the previous two years as a result of malicious acts of cyber crime. Similarly, the US based computer security institute (CSI) with the help of FBI estimated an average loss of USD 0.5 million in 2003 and USD 0.8 million in 2002. In the same way, targeted companies suffer substantial falls in stock prices estimated at about 2% immediately after an announcement of cyber crime is made (OECD, 2008). The financial impact of “virus attacks” surged from USD 2 billion in 1996 to USD 17 billion in 2000 (OECD, 2008). Among risks facing banks globally, poor risk management and fraud are ranked highly at 6 and 15 respectively out of 30 risk factors (CSFI, 2010).

The use of cyber space as a platform and catalyst for sophisticated as well as organized crimes is of concern to governments world wide. Fraud, forgery, money laundering, terrorism, as well as human and drug trafficking are all crimes that may occur through cyber networks. Furthermore, cyber crimes such as harassment via e-mail, defamation, pornography, indecent exposure and distribution of pirated software are of concern to governments given their potential for corrupting the youth and causing organizations to incur financial losses (Dombrowski, Gischlar, and Durst: 2007).

The Central Bank of Kenya has set out to promote the establishment of clearly defined risk management frameworks in individual financial institutions as evidenced by 94% of these institutions reporting to CBK in 2005 that they had defined risk management guidelines. From this number, 68% reported to have measures in operational risk while 9% had measures in IT. However, only 21% of these institutions generate adequate and consistent risk monitoring reports in addition to the returns submitted to CBK (CBK, 2005). CBK has also joined the East and Southern Africa Anti- Money Laundering Group (ESAAMLG) in order to combat money laundering and financing of terrorism in Kenya. The group

works in partnership with UNODC, World Bank, Financial Action Task Force (FATF) and both UK and USA governments (CBK,2008). Kenya Police also has standing agreements with International Police Association (Interpol) to cooperate in matters of interest. Installing anonymous hotlines and reporting mechanisms can aid in the prevention of fraud (ACFE, 2006).

Most authorities in Africa however, are hampered in combating cyber crime because some states lack internet laws and have limited internet access. Kenya similarly does not have cyber crime laws, save for section 2 of the Evidence Act (after amendment 69 of 2000) which makes a comprehensive definition of the word 'computer' for purposes of the Act. The Communication Act of 1998, Science and Technology Act Chapter 250 of 1977 and the Penal Code are the most commonly used legislation in controlling cyber crime. Defenses such as encryption policies, frequently updated virus checkers, new fire walls, access control and ID checkers are among the non-legal measures available for control of cyber crime in Kenya.

Experts however agree that it is not possible to achieve absolute cyber security due to the openness of the internet which is also associated with innovation and proliferation of programs (OECD, 2009). In the internet world, the benefits of productivity growth often outweigh the cost of innovation in security as in the case of online credit card transactions. The benefits of expanding the online activities are higher than the associated costs of the increase in fraud and as such total security is neither achievable nor desirable in many circumstances (OECD, 2009).

Unofficial reports show that in the third quarter of the year 2010, bank fraud tripled to Kshs 1.7 billion (Business Daily Correspondent, 2010b). According to BFID, majority these cases occur as a result of the banks' inadequate capacity to

take action and failure to make full disclosure for fear of bad publicity. As a result, ETR, RTGS and SWIFT transfers have accounted for the largest means of fraud (ibid). In addition to experiencing lukewarm assistance from financial institutions, the CID CCU also experiences challenges of frequent technology changes when investigating financial based cyber crimes (Aaron, 2010). This makes cyber based financial fraud to be one of the hardest to detect and prevent (ibid). The regular police and other units within CID are unable to investigate cyber crimes due to either lack of awareness that an offence has been committed or inadequate capacity in terms of skills and equipment. Considering that the measures that the banks and financial institutions adopt to prevent cyber crimes are generally delinked from routine law enforcement process, this study sought to investigate the capacity of the CID CCU to deal with cyber based financial crime in Kenya.

Despite all the advantages of the internet in making business convenient, the internet presents risks such as cyber based financial crime which is rampant in the communications and financial sectors. Statistics show that in Kenya, criminals targeted financial institutions and siphoned away an estimated Kshs. 456.3 million in the first seven months of 2009 and attempted to steal Kshs 186.7 million in the same period (Okoth, 2009). In 2008, Kshs. 913, 154, 000/= was lost in local currency in addition to the equivalent of USD 291, 000/= in foreign currency in the same year (ibid). The losses were attributed to weak computer controls in banks which could easily be overridden. These figures though unofficial, reveal the extent of fraud as reported by banks to CBK's Anti-fraud Unit. Central Bank of Kenya, banks and other financial institutions in Kenya do not make their fraud reports accessible to the public. However, international reports such as the Pricewater house Coopers Global Crime Survey of 2009 reveals that internet mediated economic crime is on the increase globally.

One of the channels that criminals use to steal from financial institutions is the EFT (EA Standard 17th November, 2009). Other money transfer services using wire applications are SWIFT, ATM applications, POS and automated clearing house applications which criminals use to steal funds directly from banks (PwC, 2009). SWIFT is a global money transfer system between banks while POS enables credit card holders to purchase goods and services. Globally, credit card use is a cyber based financial transaction which has increased over time due to the convenience, safety, social status and simplified borrowing associated with it. However, credit card use has been affected by fraud through ease in the commission of credit card offences, laxity in law enforcement efforts and inadequate laws in some jurisdictions.

Visa and MasterCard are the most common and extensively used cards in Kenya. At the point of sale, a genuine card may be skimmed for information to make duplicate cards and white plastic cards made from such data which are subsequently used to incur fraudulent expenses on the victim's account. Criminals may also make counterfeit cards by altering genuine cards especially by ironing the card then embossing a new number or re-encoding a genuine card with new details (Burns and Stanley, 2002).

Inadequate public awareness about cyber based financial crime and ineffective or non - existent laws and policies for enforcement and addressing cyber crime are among the reasons for continued proliferation of cyber crime (Granville, 2003). Others are lack of internet access, limited knowledge about the internet among users and continued growth and sophistication of technological knowledge among criminals as well as the ability of criminals to compromise bank employees and account holders (Granville, 2003).

Kenya is however at risk of losing the war against cyber crime because of the little importance placed on the issue by the government. This is in view of the existing legal tools and expertise which are inferior to the present technological and social changes (Salifu, 2008). Inadequate laws could therefore also fuel the growth in cyber crime. Increased internet and mobile phone use in banking could further fuel cases of fraud and money laundering despite the enactment of the Anti-money Laundering Act whose effect is still yet to be felt (Salifu, 2008). A solution to these problems posed by the threat of Cyber crime will therefore be individual financial institutions taking effective risk management frameworks in their operations and government enacting and strengthening enforcement of internet laws.

1.2 Problem Statement

Cyber crime is currently a major global concern given the economic losses companies incur world wide as a result of the crime. Analysts observe that cyber based financial crime thrives in Kenya even though there are institutions charged with enforcing laws pertaining to the crime. Close scrutiny of banks in Kenya reveals massive loss of money as a result of cyber based financial crime (PwC, 2009). Banks have also not been successful in protecting themselves from cyber based financial crime. Records reveal that there was an increase in the number of cases of credit card fraud from 36 cases in 2004 to 47 cases in 2007 and increase in the amount of money lost from Kshs. 400,326 in 2004 to Kshs. 10,907,152 in 2007 (BFID, 2007). Since no report has been published in the subsequent years to show a decline in incidence and impact of cyber crime in banking institutions in Kenya, it could be concluded that the adverse effects of the crime have continued to increase over the years.

In Kenya, cash transfer modes such as 'Money Gram', 'Western Union', 'Kenswitch', 'Pesa Point' and the 'M-Kesho' partnership between Equity Bank

and Safaricom have revolutionized the way money is transferred. 'Western Union' and 'Money Gram' are international modes of sending and receiving money electronically while 'Pesa Point' is an independent service provider with a network of ATM outlets in Kenya. 'Kenswitch' interconnects banks and ATMs belonging to independent service providers such as 'Pesa Point' so as to reduce the cost of delivering the service to the end user.

Like in other forms of cyber based financial transactions, institutions operating these facilities have experienced cases of fraud, although the cases have largely remained undisclosed to the public. The Cyber Crime Unit of CID headquarters which has been in operation since 2007 received 18 officers in 2009 who had undergone training on Cyber Crime in the United States of America in the same year (Daily Nation 3rd January, 2009). The CID CCU employs new technology to unearth cases of cyber based financial crime and use the evidence to prosecute offenders. This is done through the Kenya Communications Amendment Act No. 1 of 2008 and with the assistance of Banking Fraud Investigations Unit of Central Bank. Apart from dealing with fraud cases, BFIU also undertakes investigations in cyber related crimes which take place in banks. The two units complement each other and receive assistance such as information in tackling cyber crime from the rest of government. If not for its link to the Anglo Leasing Scandal¹, the proposed construction of the CID Forensic Laboratory Project could have boosted the ability of these units to effectively tackle cyber crime.

Among the key findings by the National Task Force on Police Reforms commonly referred to as the Ransley Report was that Kenya detectives were ill equipped to deal with sophisticated crimes such as cyber crime. The Report also pointed that the practice of using serving officers as forensic scientists was

¹ The Anglo Leasing Scandal involved payment of massive quantities of money by the Kenya government to non existent foreign companies for the construction of various security related projects in the years leading to the 2007 general elections.

outdated (Daily Nation 7th July, 2010). The Ransley Report identified three areas in which the law enforcement agencies were inadequately equipped to deal effectively with cyber crime. These included inadequate facilities and equipment as evidenced by the lack of laboratories and inadequate expertise as evidenced by deployment of serving officers as opposed to forensic experts to handle sophisticated crime. The other limitation was inadequate staffing as shown by ad hoc deployment of law enforcers to cyber and sophisticated crime operations. The report recommended decentralization of the police establishment to encourage professionalism, enactment of the Police Reforms Act to implement reforms and the creation of the Police Reforms Implementation Commission to institutionalize the reforms (ICTJ, 2010). Other recommendations included establishment of a Police Service Commission and the implementation of a National Policing Policy and a National Security Policy (ibid).

From the above observations it is clear that the capacity of law enforcement agencies and banks to address the growing challenge of financial based cyber crimes is limited despite the existence of some designated enforcement agencies that rely largely on the framework of the Kenya Communications Act of 1999 for their operations. This study therefore sought to assess the capacity of the Cyber Crime Prevention Unit in preventing cyber based financial crimes in Kenya.

1.2.1 Research Questions

The research questions for this study were:

- i. What are the trends in cyber based financial crime in Kenya?
- ii. What are the structures and mechanisms for cyber policing and crime prevention in financial institutions in Kenya?
- iii. What are the obstacles to the prevention of cyber based financial crime in Kenya?

- iv. What is the capacity of CID Headquarters Cyber Crime Prevention unit for prevention of cyber based financial crimes in Kenya?

1.3 Objectives of the study

1.3.1 General Objective

The general objective of the study was to assess the capacity of CID Headquarters Cyber Crime Prevention Unit in preventing cyber based financial crimes Kenya.

1.3.2 Specific Objectives

1. To examine the trends in cyber based financial crime in Kenya.
2. To identify the structures and mechanisms for cyber policing and crime prevention in financial institutions in Kenya.
3. To identify and analyze obstacles to the prevention of cyber based financial crime in Kenya.
4. To assess the capacity of CID Headquarters Cyber Crime Prevention unit for prevention of cyber based financial crimes in Kenya.

1.4 Rationale

Cyber based financial crime hurts the economy and encourages commission of more serious crimes some of which are transnational in nature. Individuals and banks in particular continue to suffer enormous losses due to cyber based financial crime which is a serious problem that calls for a combined effort for its effective control. Despite these developments, cyber based financial crime has been largely ignored by academic researchers and remains almost the exclusive domain of specialized fraud investigators and reformed con artists themselves (Langenderfer and Shimp, 2001).

The present perception as stated above is that this is an area that is only of interest to people with extensive technical knowledge and expertise in ICT. This study sought to unravel the social –economic and political dimensions of the problem and demystifying the secrecy surrounding the issue of security and finance. The Cyber Crime Prevention Unit is mandated to prevent cyber based financial crime in the country but this role has not been examined to determine the unit’s capacity to fulfill its mandate.

1.5 Scope and Limitations

This study focused on the Cyber Prevention Unit at CID Headquarters while information pertaining to cyber based financial transactions and crime risks was sourced from computer security firms, banks and other financial institutions such as those in micro-finance. Central Bank plays a key role in enforcing control measures directed at prevention of cyber based crime as well as other crimes affecting financial institutions and therefore provided important information on cyber crime.

Issues of confidentiality of cases especially with regard to individual banks and reluctance to share information about specific cases and operational procedures among CCU staff also emerged. This was overcome by obtaining appropriate permission to undertake the study and focusing on matters that were purely of academic interest.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter reviews both published and unpublished literature that are relevant to the study topic and objectives. It summarizes existing information on the risks and effects of cyber crime on financial institutions, ways of prevention of cyber crimes and obstacles to the prevention of cyber crimes. It also examines the global trends and theories in cyber space policing and financial crime detection and prevention.

2.1.1 The Role of the Internet

The internet provides many opportunities for individuals and organizations but brings with it a greatly increased information risk (Sliter, 2006). With technology and explosive growth of internet especially e-commerce, internet crime has quickly become a major concern for consumers, merchants, law enforcement, professionals and government alike (Salifu, 2008). The openness of the internet is both its best asset and worst liability. It was originally designed as a means of ensuring continued communications in the event of a nuclear war destroying the conventional telecommunications infrastructure.

According to Taylor (2000) and Vegh (2002), the internet is seen as part of the globalization process that is supposedly sweeping away old realities and certainties, creating new opportunities and challenges associated with living in a "shrinking" world. Yet awareness of, and enthusiasm for, these changes have been tempered by fears that the internet brings with it new threats and dangers to well being and security. "Cyber space" which is the realm of computerized interactions and exchanges, seems to offer a vast range of new opportunities for criminal and deviant activities. Granville (2003) argues that cyber activity is the lubricant and catalyst for sophisticated and elusive organized crimes and is also

the means by which law enforcement authorities worldwide seek new ways to stem the growth of crime. The risk of cyber crime is therefore a global issue (Salifu, 2008).

Thomas and Loader (2000) conceptualize cyber crime as those computer mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through globally created computer networks. Cyber crime poses one of the biggest threats to the widespread development and utilization of ICT around the globe (Salifu, 2008). According to Granville (2003) and Ajala (2007), Cyber crime involves the use of computers and the internet as an instrument to further illegal ends such as frauds and forgeries, theft of identities and money laundering and terrorism. They are used as a target for unlawful acts such as unauthorized access to computers or hacking and illicit tampering with files and data through unauthorized copying, modification or destruction of systems or networks and physical theft or damage of the computer.

Acts of cyber crime also include hacking or unauthorized access to computer systems or networks. Computer related fraud is the most popular and common category of all the cyber crimes and is conducted through altering computer input in an unauthorized way and disrupting or suppressing or stealing input. It also includes making unapproved changes to stored information and amending or misusing programs. The most sophisticated form of e-commerce crime is credit card fraud (Ajala, 2000).

There are some other modes of cyber crime which include e-mail bombing, data diddling, salami attacks, denial of service (DOS) attack, virus or worm attack, logic bombs, Trojan attacks and web jacking (Pati, 2008). Financial institutions are directly affected by cyber based crimes such as electronic money laundering

and tax evasion, sales and investment fraud and electronic funds transfer (EFT) fraud. EFT fraud is carried out through existing systems such as ATM, EFT and at POS technologies such as stored value cards like smart cards or super smart cards and optical memory cards (Granville, 2003).

Wall (2002a) places cyber crime in four established legal categories that:

Cyber trespasses - crossing boundaries into other people's property and/or causing damage through hacking, defacement or infecting with viruses. Cyber deception and thefts - stealing of money or property through credit card fraud and intellectual property violations. Cyber pornography - breaching laws on obscenity and decency. And Cyber violence - doing psychological harm or initiating physical harm against others.

Financial based Cyber Crime is the category of cyber crime which poses the greatest risk to financial institutions and their clients by actual loss of money through fraud. It directly affects the financial institutions' core business of safe custody of money and impacts on the customers' confidence in the institution. In this way, Financial based cyber crime is able to alter the business environment of the financial sector.

Economic factors are among the main cause of cyber crime apart from the other reasons suggested by Grabosky (2005) such as greed, lust, power, revenge, adventure and the desire to taste the "forbidden fruit". Cyber criminals are likely to be young, clever and fairly lonely individuals who are of middle class origin and often without prior criminal records. They also possess expert knowledge and are often motivated by a variety of financial and non-financial goals (Wall, 2001 in Salifu, 2008). Another group which poses a threat to internet security are insiders who range from persons who constitute insider threats ranging from

incompetent users making critical mistakes to moles who have been recruited, trained and planted by nefarious outsiders (CSTB, 2001).

2.1.2 Information Security

With the rapid growth in internet-based commerce and the complementary rise in cyber crime, information security is therefore receiving increasing attention within organizations (Ellison and Leclerc, 2006 in Pant et al, 2006). Many authors reveal that information security has historically been viewed primarily as a technical issue hence its focus has been on technological solutions (Granville, 2003; Ajala, 2007). Recent discovery has shown that information security involves a complex interaction between technical, organizational and behavioural factors (Pant et al, 2006). Current thinking is that effective infosec policies are best developed not by the IT department but by senior management in a position to take the needed holistic view of the problem (Dutta and McCrohan, 2000 in Pant et al, 2006).

Cyber security vulnerabilities fall in three main areas - the first is confidentiality whereby a secure system will keep protected information away from those who should not have access to it. Secondly, integrity ensures that a secure system produces the same results or information whether or not the system has been attacked. When integrity is violated, the system may continue to operate but under some circumstances of operation, it does not provide adequate results or information expected. Third is availability whereby a secure system is available for normal use even in the face of an attack (Goodman and Lin (eds), 2007).

Information security is concerned with unauthorized access to an organization's data. Given that almost all forms of organizational data are now stored, transmitted and processed electronically in digital form, technology is and must continue to be a central element in achieving infosec. Since organizational and

behavioral factors also play an important role, security technology can be bypassed by targeting untrained or naïve end users (Dutta and Roy, 2008). A major component of information and infrastructure security is a nation's ability to deter, detect, investigate and prosecute cyber criminal activities. Weaknesses in any of these areas can compromise security of the country and that of the world (Westby 2003 in Salifu, 2008).

2.2 Trends in Cyber Crime

2.2.1 Trends Globally

The internet's sheer size and open connectivity provides a platform to encompass the hacker community and its subculture. It is an open, interconnected communications infrastructure that is unregulated and largely unpoliced and also unpolicable (Ford and Baum, 2001 in Armstrong and Forde, 2008). The internet offers significant benefit to developing countries both for the associated development potential and for the economic, technological and cultural dividends. The internet remains a source of unlimited opportunities despite major barriers faced by these countries as a result of low literacy rates and lack of appropriate infrastructure (Salifu, 2008).

E-commerce or internet commerce is a challenging research topic because of its rapidly changing nature. It refers to any transaction completed over a computer - mediated network that involves the transfer of ownership rights to use goods or services. E - Commerce is also the carrying out of business transactions in cyber space which are in essence digitally enabled transactions (London and Guercio, Traver, 2004 in Fletcher, 2007). Online security has been shown to have weaknesses due to massive theft of online credit card records and malicious denial of service attacks (Kilker, 2000 in Grant and Meadows, 2002). The internet has enabled the development of informal banking institutions and parallel banking systems which may allow central banks' supervision to be bypassed and

therefore facilitate the evasion of cash transaction reporting requirements (Grabosky and Smith, 1998).

The E-Commerce industry is one of the critical infrastructures listed as those that are so vital that their incapacity or destruction could have a debilitating impact on the defense or economic security of the country. Others are finance, banking and telecommunications. In varying degrees, the economies of the world are driven by developments in IT (Mc Crohan, 2003). E-Commerce is threatened by a wide variety of factors including criminal hackers. Further, the commercial products supporting e-commerce have flaws while the producer advisories are frequently read and acted on by hackers before they are read and acted on by the users (McCrohan, 2003).

E-Commerce changes the competitive landscape of banking in two ways; e-commerce transactions do not require a brick and mortar branch and secondly, the internet significantly improves price transparency adding a further impetus to the commoditization of financial products and services. E-Commerce therefore has enabled multinational banking and insurance firms to expand into retail banking creating new universal banks called 'bancassurers'. Convenience of internet banking makes it particularly attractive to younger technology literate banking customers (Mols, 1999 in Wright, 2002). Among the attributes of the internet banking is the security of financial transactions (Wright, 2002).

Retail banking has been most affected by the changes in distribution channels enabled by advanced telecommunications such as the internet. The internet provides optimal advantages as a transaction and distribution medium when value propositions are intangible and frequently purchased as is the case with many banking products and services (Phan and Poon, 2000 in Wright, 2002). Advantages of the internet on retail banking include generation of cost savings

due to delegation of tasks previously performed by a branch teller, expansion of the customer base, especially among high net-worth individuals and the ability to generate revenues via cross-selling. Other advantages are mass customization which creates the perception among each individual user that the service is personalized or customized to their needs and the ability to build and utilize comprehensive customer databases and improve on bank marketing and communication via the interactive nature of the internet (Wright, 2002).

Cyber crime results in huge financial losses while frictional drag on important economic and security-related processes and other insecurities allow criminals to extract enormous amounts of money in fraud and extortion and force businesses to spend more to defend themselves against these threats. Concerns about insecurity may also inhibit the use of information technology in the future and thus lead to self denial of the benefits they bring. If consumers are not confident of online security, they will be more reluctant to engage in online activities and e-commerce hence the financial institution will suffer losses (Goodman and Lin, 2007).

The need to secure systems and push for compliance and reduce incidents of cyber attacks has driven financial institutions and SMEs to invest in internet security. At the moment, worldwide security software is forecast to surpass \$ 16.5 billion in 2010 which is a 113% increase from the 2009 revenue of \$ 14.8 billion (Business Daily Correspondent, 2010). Much of the impetus for setting minimum security standards comes from the threat of Business to Business network hackers, competitors and governments (Mc Crohan, 2003).

East Africa currently enjoys internet connectivity boom with the landing of the high speed fiber connectivity through Sea.Com. This has enabled local businesses

and security vendors to go online as a result of increased connectivity in the country (Kinyanjui, 2010).

2.2.2 Trends in Kenya

According to Kaspersky, an international data security firm, Kenya tops the list of East African countries with the highest number of security detections as a result of attacks by computer viruses. Between January and September 2010, Kenya ranked in first place with 40% security detections, Tanzania with 14% at second place and Ethiopia was third with 1.1%. Globally, Kenya has less than 1% of infections but ranks number 37 in security detections (Kinyanjui, 2010). One of the ways criminals use to compromise the security systems of financial institutions within both the intranet and internet is through computer viruses. Some computer viruses are able to circumvent protection software and can not only damage files on individual users' computers but can also bog down the internet itself by infecting web servers (Grant and Meadows, 2002).

In EAC region and specifically in Kenya, the absence of a legal framework on identity crime and related crimes such as financial based cyber crime means that enforcement personnel do not receive any specialized training (UNODC, 2010). The legal framework is inadequate with most focus directed towards retributive instead of prevention or other harm reduction policies, while some financial based cyber crimes are of a transnational nature and may be discontinued due to evidentiary or cost obstacles (ibid). There is therefore a need for a study in identity related crimes in Kenya and other parts of the world (ibid). One issue that sticks out in the foregoing is that financial institutions and state agencies such as the CID CCU are subject to different rules and requirements depending on source or location of the violation. The mandates and powers of the state agencies is to investigate and prosecute crimes as compared to companies which

have concerns about customer privacy and consequent civil liability if they disclose private information without lawful authority (UNODC, 2007).

2.2.3 The Kenya Banking Sector

Banking business and conditions of operations are governed by the Banking Act and the CBK Act in addition to Bills of Exchange Act, Companies Act, Building Societies Act and Cheques Act. The amended CBK Act of 1996 sought to promote smooth operation of payments, clearing and settlement systems (CBK, 2003). According to the CBK, electronic methods of payment include EFT, direct debits, SWIFT and customized banking services such as office-banking, home-banking, internet banking, tele-banking and mobile banking. The EFT system is used to transfer value between banks on behalf of customers and used in Kenya to process payments electronically via the automated Nairobi clearing house between KBA member banks. Direct debits allow for payments of regular bills while SWIFT, a cooperative owned by member banks in 199 countries, supplies secure and standardized financial messages. These are in addition to the other forms of payment such as cheques, payment cards or plastic money in the form of debit cards, charge cards and ATM Cards (CBK, 2003).

At the moment, CBK uses KEPSS to move volumes of transaction messages of varying values while banks use RTGS to deposit money directly into the recipient's account. RTGS requires customers to give instructions to their banks instead of writing cheques for banks to effect such payments electronically, hence reducing chances of fraud (Kasidi, 2009). Within the Kenya banking sector, several banks have adopted the use of mobile phone technology as a service delivery channel to enhance services to customers, there has been an establishment of credit information sharing mechanism and the amendment of Banking Act to permit banks to use agents in their outreach (CBK, 2010b).

Developments in ICT or electronic banking has witnessed several banks upgrading their core banking systems to either Flexicube or T 24 and these enhanced ICT platforms have enabled banks to introduce internet and mobile banking services and products. By December 2009, the number of commercial banks providing electronic banking was 33 out of 44 while 19 banks out of the 33 offered electronic overseas money transfer services in collaboration with various international money transfer agents. (CBK, 2010b).

The banking sector is comprised of the CBK as the regulatory authority, commercial banks, non bank financial institutions, foreign exchange bureaus and deposit taking microfinance institutions. As at 31st December 2009, the sector was composed of 46 institutions with 43 commercial banks and 2 mortgage finance companies. There was one licensed deposit taking microfinance institution and 130 foreign exchange bureaus. Within the 46 institutions, 13 were foreign owned while 33 were locally owned comprising of 3 banks with public shareholding, 28 were privately owned commercial banks and 2 were mortgage finance companies. The foreign owned financial institutions comprised of 9 locally incorporated foreign banks and 4 branches of foreign incorporated banks (CBK, 2010a and 2010b). This growth in banking relates directly to growth in proliferation of cyber crime as evidenced by increase in cyber based financial crime.

2.2.4 Legislation on Cyber Crime

The UN General Assembly took an early initiative to call for member states to become aware and prepare necessary legal and administrative procedures to prevent or prosecute cyber crime. Resolution (55/63) on combating the criminal misuse of information technologies adopted on 22nd January 2001 is a strong weapon for the prevention of cyber crime that calls on national governments to respond by adopting the following preventive measures by ensuring that their

laws and practices eliminate safe havens for criminals. Law enforcement cooperation in the investigation and prosecution of international cases of cyber crime should be coordinated among all concerned states. Information should be exchanged between states regarding the problems faced in combating cyber crime. Law enforcement personnel should also be trained and equipped to address cyber crime.

The Legal system should protect confidentiality, integrity and availability of data and computer systems from unauthorized impairment and ensure that cyber crime is penalized. Again Legal systems to permit the preservation of quick access to electronic data pertaining to particular criminal investigations. Mutual assistance regimes should ensure the timely investigation of the criminal misuse of information technologies and the timely gathering and exchange of evidence in such cases.

The general public should be made aware of the need to prevent and combat cyber crime. Information technologies should be designed to help prevent and detect criminal misuse, trace criminals and collect evidence to the extent practicable. The fight against cyber crime requires the development of solutions taking into account both the protection of individual freedoms and privacy and the preservation of the capacity of governments to fight such criminal misuse (Ajala, 2007).

In Kenya, the Crime and Anti-Money Laundering Act of 2009 or AML Act of 2009 was passed by Parliament on 10th December 2009 and is divided into several parts. Part 3 outlines the guidelines in the formation of a financial reporting centre, Part 4 deals with the anti money laundering obligations of reporting institutions. Part 12 outlines international mutual legal assistance in investigations and proceedings between Kenya and other countries in

investigation of offences or enforcement of orders. Similarly, Part 13 entails miscellaneous proceedings such as miscellaneous provisions relating to the conduct of investigations, access to information and admissibility of electronic evidence among others (CBK, 2010b). The National Taskforce on Anti-Money Laundering and Combating the financing of Terrorism (CFT) was established and gazetted in April 2003 with the mandate of establishing a comprehensive AML/CFT regime in Kenya focusing on AML. The Taskforce has also partnered with the UNODC Nairobi office.

2.3 Structures and Mechanisms to Prevent Cyber Crime in Financial Institutions

Various countries use legal, organizational and technological approaches to fight cyber crime. The legal approach aims to restrict cyber criminal activities through legislation; the organizational approach aims to enforce laws to promote cooperation and to educate the public through the establishment of dedicated organizations. The technological approach aims to increase the effectiveness and efficiency of cyber crime analysis and investigation with the help of new technologies (Chunga et al, 2004 in Salifu, 2008).

2.3.1 Legal Framework

According to Wilson (2005), one important area that the governments in the world need to take into consideration is internet governance due to the fact that good governance of the use of internet to a high degree considerably lowers the cyber crime level. According to IT expert Sean Siochru, governance is a set of processes that are employed to assess, weigh, and balance the different (and possibly competing) values and objectives inherent in society's diverse interest and actors. Developing countries must enact laws that criminalize the use of computers, access devices and the internet for criminal purposes. However, the laws defining computer offenses and the legal tools needed to investigate

criminals using the internet often lag behind technological and social changes, creating legal challenges to law enforcement agencies (Salifu, 2008).

The enactment of the Anti-money Laundering Act in addition to supporting the establishment of the Credit Reference Bureaus will reinforce commitment by commercial banks to minimize fraud through sharing of information on irregular transactions. KBA is working with others to implement new systems expected to eliminate risks through establishing a new cheque truncation system which enables banks to send images instead of paper cheques for clearing and settlement. KBA is also exploring ways of facilitating the establishment of a fraud management system, strengthening the investigative capacity of CBK's BFIU and enhancing judicial consequences of fraud (Njunguna and Etemesi, 2010).

Internet specific regulation is required to combat growth of financial fraud in cyber space and the law therefore needs to be modernized to deal with the technological changes while cyber criminals have become more sophisticated hence technology must imitate this sophistication (Logica, 2004). What is required is any form of regulation which will need to specifically target the weaknesses that assist criminals in carrying out online fraud. These weaknesses include anonymity in cyber space and cyber jurisdiction to deal with challenges of jurisdiction that financial fraud in cyber space creates (Fletcher 2007). Menthe (1998) and Johnson and Post (1996) have called for cyber space to be treated as a separate jurisdiction. This would be a welcome future development to the legal framework.

Enough evidence should be collected for prosecution of online financial fraud since international nature of cyber space is a difficult issue as far as jurisdiction is concerned since we are concerned with ensuring that a legal framework is in

place that allows law enforcement agencies or other agencies to cooperate in the fight against financial fraud in cyber space (Fletcher, 2007). An important trend in contemporary policing seems to be the shift towards intelligence-led policing (Heaton, 2000, Cope 2004) which allows police agencies to better understand their crime problems and take a measure of the resources available to be able to decide on an enforcement tactic or prevention strategy best designed to control crime.

Intelligence led policing advocates for a proactive approach which includes decision makers wanting to be informed about significant and emerging challenges and threats to anticipate, plan and take appropriate preventive action and target their crime control efforts better (Verfaillie and Vender Beken, 2008). Among the recommendations for business to business firms (B2B) in carefully managing their information security posture are the managerial recommendations whereby the firm will face for profit hackers, organized crime, the technologically sophisticated virus developer as well as their employees apart from many others. They therefore need to protect themselves by addressing their external and internal environments (Mc Crohan, 2003).

2.3.2 Human Resources

When cyber crime reaches the level of organized crime, the solution is in integrated policing philosophy which involves all levels of law enforcement working cohesively with each other, exchanging strategic and criminal intelligence, sharing tactical and operational knowledge, planning joint and individual actions and communicating effectively (Sliter, 2006). An example is Canada's Integrated Market Enforcement Team (IMETs) whose aim is to deter perpetrators of crimes by ensuring there is a genuine risk of being discovered, prosecuted and incarcerated (Sliter, 2006).

Broadhurst (2005) contends that effective control of cyber crime requires more than cooperation between public and private security agencies. The role of the communication and IT industries in designing products that are resistant to crime and that facilitate detection and investigation is therefore crucial (Overill, 2003). Since cyber crime affects all businesses, governments and citizens, the classical Three-layer security paradigm is made up of protection, detection and reaction which has traditionally been applied to the information assurance with firewalls playing a major protective role while detection is handled mainly by intrusion detection systems (Overill, 2003).

Measures to reduce crime risk must be used in combination with self protection since there is a weak state of global legal protections hence personal awareness of cyber crime methods and measures for self protection of self and organization are important. This is through good knowledge of effective antivirus and lookout for “too good to be true” offers since greed and unrealistic expectations motivate most victims. Secondly, effective laws by government through enactment of enforceable computer crime laws that also respect the rights of the individuals. Thirdly, firms, government and communities must work together to strengthen their legal framework on security against cyber crime through awareness and knowledge (Ajala, 2007).

Law enforcers must be properly trained, must be technologically sound enough to handle such crimes and apply proper strategy in issues of enforcement. That is, by avoiding harassment, abuse of privacy and extortion and not to punish genuine users or frustrate them and make them to be unable to benefit from the internet. Strategies must therefore be made to strike a balance between security concerns and other developmental needs. Thus, international comprehensive cyber laws coordinated by an international coalition body should be in place so as to leave no country a hiding place for cyber criminals (Ajala, 2007).

There are five main levels of regulations or safeguards at which regulation takes place on the internet. These are users, ISPs, corporate security organizations, state-funded non-police organizations and state-funded public police organizations (Wall, 2001). In line with the above, there are three legal principles that need to be considered as safeguards for determining the applicable jurisdiction in issues relating to cyber space. These are the territoriality principle which would enable a country to order those ISPs operating in its territory. Secondly, the nationality principle is the right of a country to regulate the conduct of its citizens anywhere in the world and thirdly, is the effects principle in which an act committed in one country causes injury in the territory of another country. It would be justifiable to have some form of legislation to compel businesses to report when they become victims of cyber crime and in return the authorities to keep the identity of the victim secret (Fletcher, 2007).

2.3.3 Technical Resources

Enhanced security requires enhanced reliability and stability and not quick fixes since criminals endeavor to find new vulnerabilities (Financial Services Authority, 2007, in Fletcher, 2007). Financial crime is an area where it is difficult to determine the exact value and frequency of occurrence as it is difficult to measure hence difficult to combat by law enforcement agencies (ibid). In determining what techniques are most appropriate in defending against the insider threat, the following three dimensions require consideration. First and foremost is the individual's access privileges, their intent and their technical abilities. There is therefore need for better training and security awareness education especially in the case of the unwitting insider or the incompetent user. Others are better authentication and access control techniques, biometrics and application based audit trails (CSTB, 2001).

Knowledge in internal controls in accounting could be employed to address human vulnerabilities that contribute to information in security (Dutta and Roy, 2008). The UN Commission on Crime Prevention and Criminal Justice in May 2001 proposed international cooperation to combat transactional crimes such as cyber crime through the use of technologies that supported criminal activities. Examples of these technologies are firewalls and encryption software to shield criminal communications from interception or intrusion just as effectively as to protect legitimate communication (CCP, 2001 in Armstrong and Forde, 2008).

Police and security officers need to learn how to locate electronic evidence and deal with cross-border issues in tracing suspected hackers or crackers. Policing of cyber space calls for concerted efforts of internet service providers, global interest groups, hotline providers and private security firms set up to protect business and individual internet users as well as government and e-business companies (Salifu, 2008). The impact of cyber crime is worst in developing countries where the technology and law enforcement expertise is inadequate (Salifu, 2008). Lack of appropriate expertise presents barriers to effective policing of cyber crime since investigation of such crimes will often require specialized technical knowledge and skills, and there is at present little indication that the police in Kenya have the appropriate training and competence (Wilson, 2005).

Gathering evidence about a computer or network crime requires expertise that is often difficult to acquire in a corporation and that often does not exist in the police or in attorney's offices. Even if a case can be constructed, the technical evidence is often too abstract or complex for juries to understand while jury sympathies are often not with the victim since most information crimes do not result in bodily harm and the asset is not "physically" lost to the victim (Vegh, 2002). Computer based evidence can be modified without an audit trail of the modifications hence crucial evidence may be inadmissible, or at best subject to

doubt. Prosecutors find it difficult to prove guilt “beyond reasonable doubt” and are not likely to take the case at all hence effective deterrent penalties are difficult to formulate because of the low probability of prosecution. Similarly, expected penalties are low and made lower by discounting over time, in view of the long and tortuous route to detection and prosecution of computer crime (Taylor, 2000).

But even with the proposition for government to take internet governance seriously the greatest challenge has been how to balance government and law enforcement need with privacy expectations. Armstrong and Forde (2008) contend that individual rights to privacy may have to be subdued in an effort to reduce cyber crime and the use of internet for criminal activities. Internet security will depend on efforts of a wide range of institutions as well as on degree of self-help by potential victims of cyber crime. The ideal configuration for a solution will entail a mix of law enforcement, technological and market solutions. Internet’s globalized nature requires effective counter measures to a substantial degree of international cooperation (Grabosky, 2005).

According to Mc Crohan (2003), externally, commercial organizations need to ensure in the public arena that they are included in programs and exercises that various government agencies conduct to assess and eliminate significant vulnerabilities to information warfare attack. They should also play a role in the legislative and regulatory process, expressing their concerns to the appropriate elected and administrative officials. They also need to know the linkages that support its ISPs as well as their security practices. It’s of little value if the firm itself has seriously considered physical and system security if they are networked with other organizations that are less concerned with security.

Internally, organizations should develop a culture of information security to include the non-cyber and cyber aspects of security and inherent in this process is leadership of senior management in information assurance. Only senior executives can address the resolution of many of these threats and one method of addressing this problem is by active engagement of executives in the conduct of vulnerability assessments (VA) to identify system weaknesses. VAs communicate the message that security is important to the organization and it is a proactive method of identifying vulnerabilities and can also be an excellent method of validating the security of outsourced systems development work (Mc Crohan, 2003).

Additionally, formalized guidelines for damage assessment in the enterprise that a system has penetrated should be developed and particular care must be taken with temporary workers. If using these workers, particular care should be established to compartmentalize them using dedicated systems and restrict prohibitions against password sharing and the use of personal disks. Managers should be fully in charge of IT security in order to address the need to determine the optimal allocation of staff or for outsourcing and consulting for information security (Olkowski, 2001).

According to Olkowski (2001), the positive outcomes as a result of the above recommendations include such benefits as the involvement of senior management and information assurance personnel who will therefore have fewer difficulties in their relationships with other areas of the firm. Secondly, the firm will be in a position to assess and eliminate significant vulnerabilities to its critical information systems. Thirdly, robust systems and procedures for detecting attacks will allow for an initial assessment of the change, an immediate warning to system users and the isolation of the affected components. Fourthly, they should minimize time lost to system failure since the overall value of such

Internally, organizations should develop a culture of information security to include the non-cyber and cyber aspects of security and inherent in this process is leadership of senior management in information assurance. Only senior executives can address the resolution of many of these threats and one method of addressing this problem is by active engagement of executives in the conduct of vulnerability assessments (VA) to identify system weaknesses. VAs communicate the message that security is important to the organization and it is a proactive method of identifying vulnerabilities and can also be an excellent method of validating the security of outsourced systems development work (Mc Crohan, 2003).

Additionally, formalized guidelines for damage assessment in the enterprise that a system has penetrated should be developed and particular care must be taken with temporary workers. If using these workers, particular care should be established to compartmentalize them using dedicated systems and restrict prohibitions against password sharing and the use of personal disks. Managers should be fully in charge of IT security in order to address the need to determine the optimal allocation of staff or for outsourcing and consulting for information security (Olkowski, 2001).

According to Olkowski (2001), the positive outcomes as a result of the above recommendations include such benefits as the involvement of senior management and information assurance personnel who will therefore have fewer difficulties in their relationships with other areas of the firm. Secondly, the firm will be in a position to assess and eliminate significant vulnerabilities to its critical information systems. Thirdly, robust systems and procedures for detecting attacks will allow for an initial assessment of the change, an immediate warning to system users and the isolation of the affected components. Fourthly, they should minimize time lost to system failure since the overall value of such

programs is that these activities improve the ability of the firm to communicate, educate, detect, react, repair, restore integrity and restrict productivity losses due to a system attack. In the event of down-stream losses due to a cyber attack, the organization will be in a position to protect itself against charges of negligence.

2.4 Obstacles to Prevention of Cyber Crime

A major problem for the study of cyber crime is the absence of consistent current definition, even among law enforcement agencies charged with tackling it (NOP/NHTCU 2002). As Wall (2001a) notes, the term has no specific referent in law yet it is often used in political, criminal justice, media, public and academic discussions. He also suggests that instead of trying to group cyber crime as a single phenomenon, it might be better to view the term as signifying a range of illicit activities whose common denominator is the central role played by networks of information and communication technology (ICT) in their commission.

Credit card fraud is on the rise in the African continent, especially in Egypt, South Africa, and Kenya. Apart from South Africa, not much research which documents evidences and studies on cyber crime has been done in Africa. It should be noted that South Africa is the only country in Africa to have documented studies on cyber crime and have also established a unit to tackle the crime. South Africa is well known for its high crime rate but should be a model for other countries in Africa on how to tackle cyber crime (Wilson, 2005). In Kenya no serious studies have been done except for mentions of cyber crime in reports and seminars.

Threats to e-commerce will continue to grow due in part to proliferation of hacker websites as well as the lack of serious emphasis on information security on the part of senior managers. Lack of attention to information security is due in

part to the rush to market mentality of the dot.com economy, the complexity of legacy systems as well as continuing difficulty of relating security to profitability. Surveys indicate that both consumers and commercial users are in doubt concerning the security of the basic systems hence are potential threats to expansion of e-commerce (McCrohan, 2003).

Cyber criminals are able to exploit three security vulnerabilities either by hacking or through the use of malicious code to gain the information required to carry out fraud. These points of vulnerability are the client, server and the communication pipeline. (Landon and Guersio Traver, 2007 in Fletcher, 2007). Cyber systems must therefore be made more stable and reliable to prevent vulnerabilities (Sofaer and Goodman, 2001 in Fletcher, 2007). This is an ideal position but is also fictional since vulnerabilities will always exist. The challenges of regulating financial fraud in cyber space are more complex than regulating fraud in the real world hence to prevent it, the use of both conventional legal responses and novel technological approaches will need to be utilized (Grabosky et al, 2009 in Fletcher, 2007).

In spite of the huge cost that computer fraud exerts upon individuals and organizations, computer fraud such as consumer fraud has been largely ignored by academic researchers hence remaining almost the exclusive domain of specialized fraud investigators and reformed con artists (Hangenderfer, 2009). Within the business to business (B2B) environment, there appears to be the realization that communication and stable security standards for companies doing business with each other over the internet area are a precondition for the safety of all of the others on the network. Information sharing between public and private sectors is an immediate need and responsibility to be shared between the two sectors (Mc Crohan, 2003). At the moment, information sharing between public and private sectors is not taking place at levels which can assist the fight

against cyber crime and is limited to the Proceeds of Crime and Anti-Money Laundering (AML) Act and the Banking (Credit Reference Bureaus) Regulation of 2008. The former came into effect in June 2010 and aims to identify, trace, seize and confiscate proceeds of crimes. The later was operationalised in February 2009 and tasks Credit Reference Bureaus to collect, manage and disseminate customer information to lenders and also enable lenders and businesses to reduce risk and fraud (CBK, 2008).

According to the Financial Services Authority (2004) in Fletcher (2007), commercial fraud including cyber based financial crime is difficult to measure which makes it extremely hard for law enforcement agencies to be able to combat it. Once the criminal activity has been detected, many businesses are reluctant to lodge a report due to fear of adverse publicity or loss of good will, embarrassment, loss of public confidence, investor loss or economic repercussions (Ajala, 2007). Another reason why firms like banks fail to report cyber attacks is lack of confidence in the ability of the police to deal with such crimes (Salifu, 2008). According to Taylor (2000), estimating economic, social and political impacts of cyber crimes and web attacks to a reasonable level of accuracy is a challenge. One view is that since many web attacks go unreported, such impacts tend to be underestimated. The opposite argument is that there may be vested interests among security companies to exaggerate the level of cyber crimes.

Internet investigations often transcend national boundaries and this creates problems to investigators since procedural laws that govern the conduct of criminal investigations are territorially based. Cyber crime poses a challenge to the society since it can be committed at any time, anywhere and authorities need to spend more time and effort compared to traditional crimes in locating and detecting offenders (Salifu, 2008). Cross border issues beset investigations as in

credit card fraud where victims and suspects are scattered around the globe. Some countries do not have laws that would capture online fraud while some compete among themselves on who to take the lead in investigations. Enforcement agencies are therefore not able to respond effectively to cyber crime and play “catch up” with cyber savvy criminals in some cases (Sussman, 1999 in Salifu, 2008).

The fast operational speed of today’s computer systems makes criminal activity difficult to detect while law enforcers often lack the necessary technical expertise to deal with criminal activity. The challenge of pinpointing responsibility on a party is another challenge that is anonymity in cyber space (Fletcher, 2007). Even if businesses are able to stay abreast with technology, it is not sufficient as every year, new internet security vulnerabilities emerge. The challenge of cyber crime is how to regulate a technology that permits rapid transactions across continents and hemispheres using legal and investigative instruments across borders (Fletcher, 2007).

Software tools for hacking all types of computer and communications systems are readily available on the internet and most can be downloaded at no or little cost (Armstrong, 2003). Online fraud creates problems to enforcement agencies internationally such as the pinpointing the victim of the fraudster between the client and the bank, identifying the party responsible for the fraud and ascertaining the party supposed to have better security systems to avoid fraud in case the fraudster cannot be identified and caught (Salifu, 2008 and Fletcher, 2007). Another challenge created by online fraud is the question of the responsible party for jurisdiction since cyber space is a place where messages and web pages are posted for everyone in the world to see if they can find them (Menthe, 1998 in Fletcher, 2007).

Questions as to the applicable laws also arise since it has to be determined which among the laws such as where the web, ISP or user is located or whether all the laws are applicable. Another challenge brought about by online fraud is in gathering of evidence required for prosecution. This is because certain cyber crimes are not recognized by some countries. Even if a victim can establish that there has been some non-compliance with laws, the problems associated with taking legal action are considerable and are not limited to the world of electronic commerce (Grabosky et al 2001 in Fletcher, 2007). Other problems created by online fraud are that it leaves no paper trail of evidence and it is problematic to quantify the extent to which deceptive and misleading practices take place online (Fletcher, 2007).

Developing countries tend to lack the infrastructural, economic and socio-political framework for development of electronic-commerce in comparison to developed countries (Salifu, 2008). Controlling cyber security also lies beyond the capacity of contemporary law enforcement and regulatory agencies (Grabosky, 2005 in Salifu, 2008). Information sharing between the public and private sectors is an immediate need and responsibility to be shared between the two sectors. However, the essence of the difficulty facing both sectors is that the economy has been on interconnected systems that were not developed to withstand coordinated technological attacks. (Mc Crohan, 2003).

2.5 Theoretical Framework

A sociological theory is a way of making sense of a disturbing situation or a phenomenon to allow us most effectively understand that phenomenon (Francis, 1982). Another writer, Kerlinger (1964) describes a theory as a set of interrelated constructs or variables, definitions and propositions that represent a systematic view of a phenomenon by specifying relations between variables with the purpose of explaining natural phenomena.

2.5.1 Control Theory

According to Giddens (2000), Control Theory posits that crime occurs as a result of an imbalance between impulses towards criminal activity and the social or physical controls that deter it. It is assumed that people act rationally and that, given the opportunity, everyone would engage in deviant acts. Many types of crime are as a result of situational decisions or opportunities motivating persons to act.

Travis Hirshi (1969) argued that humans are fundamentally selfish and make calculated decisions about whether or not to engage in criminal activity by weighing the potential benefits and risks. Bonds hold people to society and good behaviour and when strong, they maintain social control by binding people not to commit crimes but if weak, delinquency and deviance occurs.

Some control theorists see the growth of crime as outcome of the increasing number of opportunities and targets for crime in modern society. The presence of goods of value and absence of restrictions offers an opportunity for committing crimes. Target hardening offers a way of preventing such crimes through taking practical measures to control the criminal's ability to commit crime. Control theory is linked to an influential approach to policing called the *theory of broken windows*. The proponents of this theory were Wilson and Kelling (1982) who suggested that there is a direct connection between the appearance of disorder and actual crime. If a single broken window is left unrepaired, it sends a message to potential offenders that neither police nor local residents are committed to the upkeep of the community. As time goes by, more signs of disorder will occur such as graffiti, litter and vandalism.

Cases of cyber based financial crime occur and increase gradually as stakeholders fail to stem the problem. Initial success for criminals leads to subsequent commission of the crimes until effective measures are put in place.

Relevance of the Theory

Criminals using cyber space to steal from financial institutions and individuals succeed due to the opportunities that are available and the low risk of arrest that they perceive. The absence of effective structures and mechanisms for cyber crime policing and prevention encourages financial based cyber crime to be perpetrated more by criminals taking advantage of lax laws and ineffective enforcement agencies. This is expected to continue until there are stringent laws in place and the agencies gain adequate capacity to counter the crime.

2.5.2 Rational Choice Theory

Among the proponents of this theory are Talcott Parsons and James Cohen. According to Parsons, action is rational in so far as it pursues ends possible within the conditions of the situation by the means which, among those available to the actor, are intrinsically best adapted to the ends. The actor knows the facts of the situation in which he acts and the conditions necessary for the realization of his ends or goals (Wallace, 1969).

According to Cohen, persons act purposively toward a goal which is shaped by values and preferences (Ritzer, 1992). In application of the Theory to criminology, criminals evaluate the risks of apprehension, the seriousness of punishments and the potential value or gains they are likely to derive from engaging in criminal activities (Siegel, 1995, Cornish and Clarke, 1986). The decision to commit crime is therefore a matter of personal choice based on weighing of the available opportunities and risks. It therefore follows that if criminal behavior is rational, then imposing heavy penalties and making it

difficult to commit crime can control it (Siegel, 1995). Criminals who engage in cyber based financial crime consider the risks of apprehension to be low and are at the same time aware of weak penalties imposed for these crimes. This acts as motivation for the commission of more crimes.

Relevance of the Theory

Criminals who engage in cyber based financial crimes are motivated by the financial gains that are there to be received. They know the extent to which they can indulge in the crime so as to avoid arrest and at the same time receive the most gain from their activities.

2.5.3 Social Systems Theory

The main proponent of this theory was Talcott Parsons who in 1960 viewed society as a system made up of separate parts called sub-systems whose failure would mean failure of the entire system hence society. This theory explains the relationship between these subsystems of the society to be based on information exchange (Ritzer, 1988).

According to Parsons (1979), a system such as a society must fulfill roles such as adaptation which entails the ways geared towards restoration of a distorted equilibrium brought about by lack of order and integration which entails facilitation of parts towards a harmonized interrelationship. Other roles are pattern maintenance whereby the society must ensure that its essential characteristics are maintained and goal attainment whereby emphasis is on motivating members to perform their roles such as heeding advice on how to live. The society should therefore aim at attaining its goals.

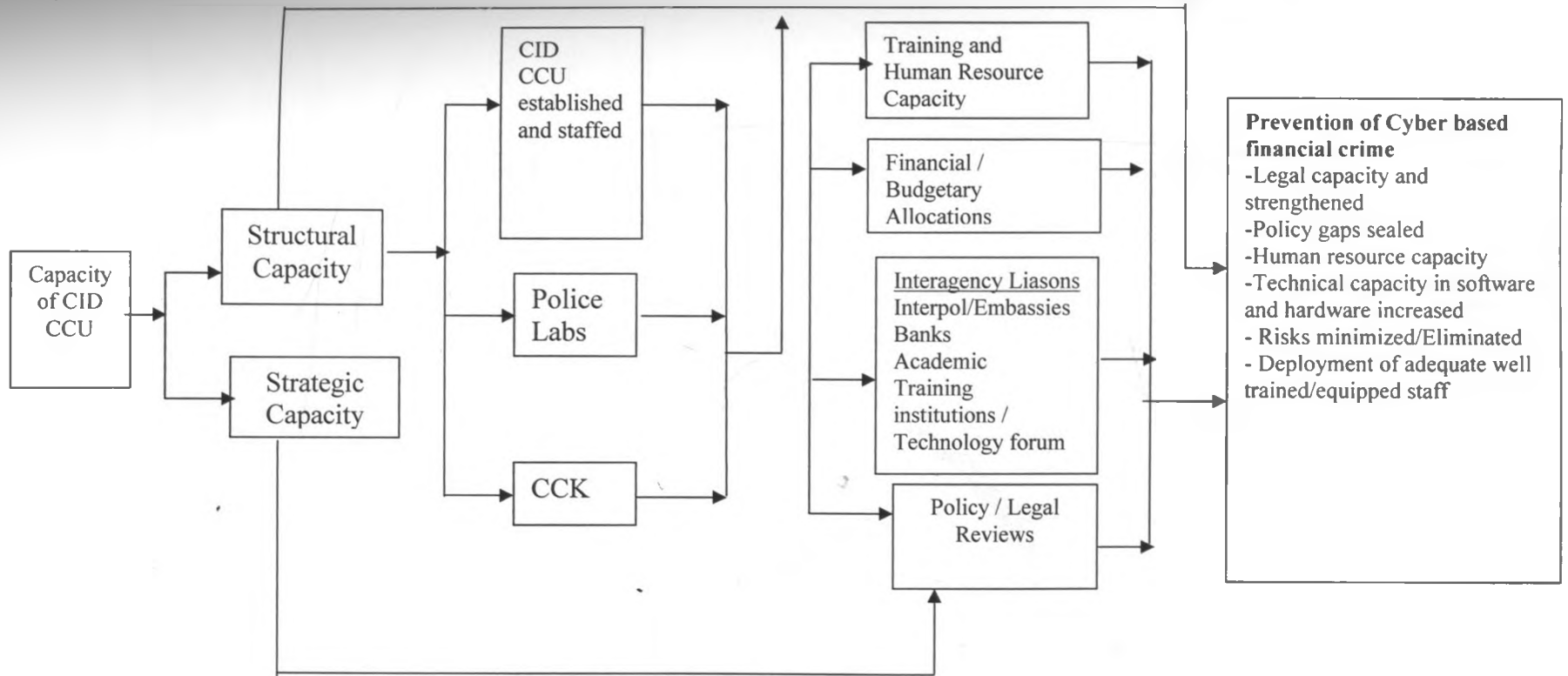
Relevance of the theory

Cyber based financial crime encompasses different parties like the criminal who commits the crime, the victim to the crime, the financial institution concerned, the internet provider and the law enforcement agencies investigating the same crime. Victims of cyber based financial crime and the different players seek to find ways of preventing the cyber based financial crime. The ultimate adoption of internet safety measures will enable these parties to eventually play their rightful roles in the internet community and in the society as a whole. However, lack of collaboration and cooperation between financial institutions such as banks, private and public cyber crime investigation agencies such as KPMG, Price Waterhouse Coopers, Kenya Institute of Data Forensic Systems, CFE and Security Risk Solutions Limited on one hand and CID CCU, Anti Terrorist Police Unit and BFID on the other has been a drawback in the fight against cyber based financial crime.

2.6 Conceptual Framework

Figure 2 shows that the capacity of the CID CCU is enhanced when the structural and strategic capacities are developed and positively utilized for the prevention of cyber crime. The structural capacity includes establishment of CID CCU and Police laboratories and involvement of CCK. The strategic capacity includes training, human resource capacity, adequate financial and budgetary allocations and technology updates. Others are inter agency liaisons including Interpol, banks, academics, technology forums and the inclusion of policy and legal reviews. This would boost the capacity of the CID CCU to prevent cyber crime in Kenya and the result will be prevention of financial based Cyber crime. However, these structural and strategic capacities seem inadequate to the extent that there is high prevalence of financial based cyber crime in Kenya.

Figure 1: Capacity of CID CCU for Prevention of Cyber Based Financial Crimes



The study therefore strove to look into CCU structures, strategies and their effect on the prevalence of cyber based financial crimes. It brought forward two Hypotheses as follows:

Ho Ineffective CCU Structures and Strategies have led to inadequate prevention of cyber crime in Kenya.

H1 Effective CCU Structures and Strategies have led to adequate prevention of cyber crime in Kenya.

CHAPTER THREE

RESEARCH METHODOLOGY

This chapter outlines the research design used, the site, population of the study, sample size and selection and the method of data analysis that was applied.

3.1 Research Site

The site of the study was CID Headquarters Cyber Crime Unit which is located within CID Headquarters in Mazingira House along Kiambu road. The site was purposively selected because it is an arm of CID mandated with investigation of cyber based financial crimes, arrest and prosecution of offenders. It is also one of the newly formed units within the Kenya Police and came as a result of the changing crime trends in areas such as cyber crime which is a popular white collar crime perpetrated through information technology. Since it is a case study of the Cyber Crime Unit (CCU), it was distinguished by intensive study of a single organization or institution and other sites outside the unit were only considered as incidental sites. The primary data was collected from 32 CCU officers while additional information was sought from 4 bank officials, a member of the judiciary, a CCK official, an official of the Computer Society of Kenya and 3 computer forensic experts. Secondary data was also analyzed to complement the data from the field.

3.2 Research Design

This study was a Case Study and used Survey Design in which the variables internet safety mechanisms and extent of cyber based financial crime were operationalized so that they could be measured. A sample was selected from the population and from which data was collected and analyzed. The research largely generated and utilised qualitative data and was concerned with the subjective assessment of the respondents' attitudes, opinions and behavior.

3.3 Units of Analysis and Observation

According to Singleton et al (1988) the unit of analysis is that which the researcher wishes to study, understand or explain. The unit of analysis for this study was capacity of CCU in prevention of cyber based financial fraud. The unit of observation is the element or aggregation of elements from which information is collected (Singleton et al, 1988). The unit of observation in this study was the CID Cyber Crime Prevention Unit.

3.4 Sampling Design

A sample is a small group of individuals obtained from an entire group or accessible population having a common observable characteristic (Mugenda and Mugenda, 1999). Sampling is therefore a process of selecting a sample from a population to become the basis for predicting the prevalence of an unknown piece of information, situation or outcome regarding the population (Kumar, 2005). The CCU was selected purposively since it deals with cases of cyber crime such as financial based cyber crime. It is a unit within the CID which is headed by the Director of Criminal Investigations (DCI) and has three branches namely the investigation branch, administration and operations branch. The investigations branch has five sections namely Serious Crimes Unit (SCU), Anti Narcotics Unit (ANU), Economic Crimes and Commercial Unit (ECCU) and Banking Fraud Investigations Unit (BFID). The CCU falls under the Serious Crimes Unit.

Sampling validation method was used to select the sample of the officers from the CID CCU work roll register. Each of the officers was selected according to his or her relevance in the prevention structures and strategies undertaken by CCU in prevention of cyber crime in general with emphasis on financial crime. This included length of service in the Force and in the CCU, work experience and any specialized knowledge on financial based cyber crime. A total sample size of 32

officers attached to CID CCU was used for the study. These officers are tasked with the exclusive investigation of cyber crimes and compose almost the entire population of the unit with the exception of the officer in charge. This was therefore an appropriate sample for the study.

To enrich the information received from the 32 respondents, 12 key informants were selected purposively. These included first, 4 bank officials from Barclays Bank of Kenya, CFC Stanbic Bank, NIC Bank and Kenya Commercial Bank. Secondly was a magistrate from the judiciary, a CCK official and an official of the Computer Society of Kenya. Third, there were 4 specialists from the computer forensic firms of Price Waterhouse Coopers, Certified Fraud Examiners (CFE-Kenya Chapter), Kenya Institute of Data and Forensic Systems and Security Risk Solutions Limited. In addition, the researcher interviewed the deputy officer in charge of the Anti Terrorist Police Unit.

3.5 Tools and Techniques of Data Collection

This study was both qualitative and quantitative whereby the data was collected by the use of tools namely structured questionnaire containing open and closed ended questions, an interview guide, a checklist and field notes. The questionnaires were administered on the 32 officers by the researcher who recorded the responses immediately they were made. The techniques that were used include document analysis of policy papers, strategic plans and official research documents to collect basic data on the research questions. Other techniques used were informal in-depth interviews administered on the 9 key informants.

3.6 Data Analysis

The collected data in form of the completed questionnaires and field records underwent editing to detect and correct errors and omissions. It was then put in

categories or classes through coding or classification according to the study's objectives and then tabulated.

The above response data was presented in tabular form, after which the researcher analyzed the data using Microsoft Excell and SPSS computer packages. The researcher then drew statistical inferences to form basis of the study findings through computation of percentages and distribution tables.

CHAPTER FOUR

DATA ANALYSIS, INTERPRETATION AND PRESENTATION

4.1 Introduction

The main purpose of this study was to assess the capacity of CID Headquarters Cyber Crime Prevention Unit in preventing cyber based financial crimes Kenya. The sample for the study included 32 respondents selected from the Cyber Crime Unit at the CID Headquarters. This chapter reports on the results of analysis of data and its presentation covering the respondents' background information, the trends of cyber based financial crime in Kenya and the structures and mechanisms for cyber policing and crime prevention in financial institutions in Kenya.

The chapter also looked into the obstacles to the prevention of cyber based financial crime in Kenya and the capacity of CID Headquarters Cyber Crime Prevention unit for prevention of cyber based financial crimes in Kenya. The findings of the study are presented using frequency distributions presented in tabular form.

4.2 Background information

This section presents the background information for the respondents detailing their demographic data, length of service both in the Police Force and in CID CCU and the highest educational attainment by the respondents.

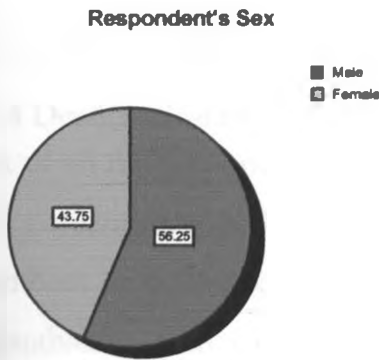
4.2.1 Distribution of Respondents

The entire CID CCU was covered in the study and all the officers attached to the unit were interviewed. This implies that this study was inclusive and a good representation of the entire population of the CID CCU site.

4.2.2 Gender of Respondents

Of all the respondents, 18 or 56 percent were male while 14 or 44 were female. This difference is attributed to the high numbers of male police officers who comprise the bulk of those who are recruited to join the Police force and eventually find their way into the unit. Another reason for this skewed distribution is that the CID CCU handles assignments related to information technology which is perceived as intellectually challenging. This attracts more male than female officers hence the composition of the unit. The sizeable number of female officers can be attributed to gender affirmation within the force which seeks to ensure equity in these postings. The difference is however marginal to affect gender representation which was therefore accurately observed.

Figure 2: Respondent's Sex

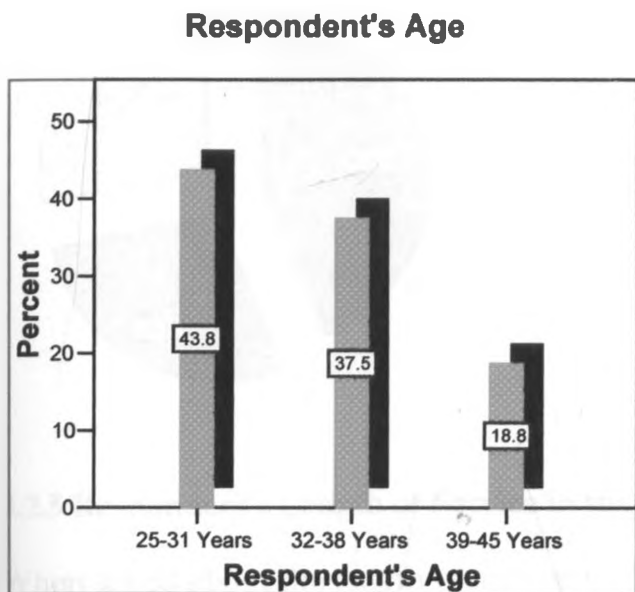


4.2.3 Age of Respondents

Figure 4 shows that 14 or 43.8 percent of the respondents were between the ages of 25-31 years, 12 or 37.5 percent fell between ages 32-38 years while only 6 or 18.8 percent of the respondents were between the ages of 39-45 years. It can be deduced therefore that the respondents had enough experience to participate in the study. It can also be deduced that CCU attracted mostly youthful officers who are interested in information technology and have passion for challenging

assignments such as those to be found in CCU due to the rapidly changing technologies.

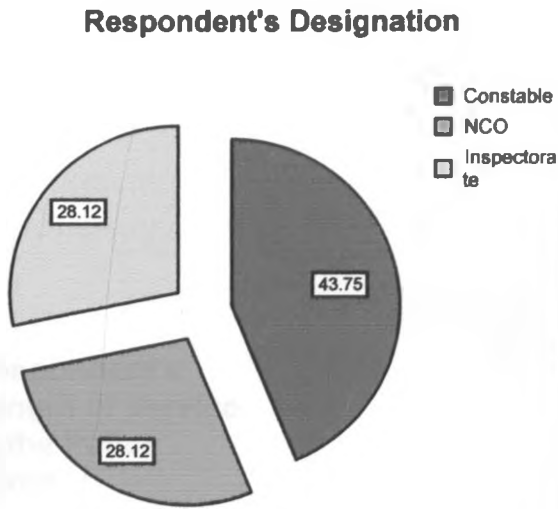
Figure 3: Respondent's Age Category



4.2.4 Designation of Respondents

Out of all the respondents, 14 or 43.8 percent were of the rank of Constable, 9 or 28.1 percent were NCOs while another 9 or 28.1 percent of the respondents were members of the inspectorate. It can be deduced that the high number of police constables within CCU is due to the corresponding high number of young officers who have recently graduated from college with relevant qualifications and have just begun their careers. The other ranks of NCO and part of inspectorate form the recently promoted young officers while a small number of the inspectorate composes those specifically brought in for the purpose of supervising the rest of the personnel.

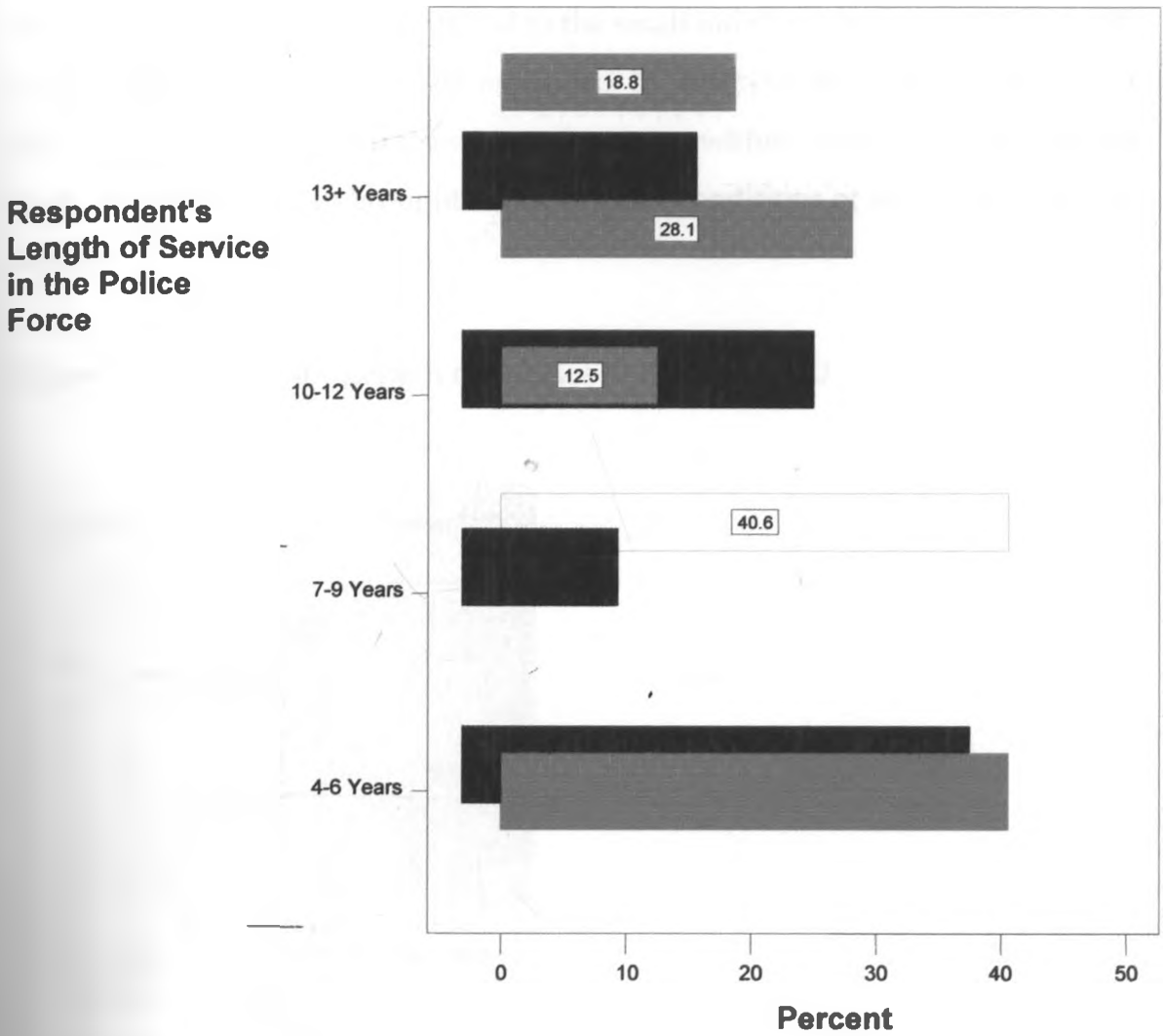
Figure 4: Respondent's Designation



4.2.5 Respondent's Length of Service in the Police Force

When asked about the length of service in the Police Force, 13 or 40.6 percent of respondents indicated that they had served in the force for a period of between 4-6 years while 4 or 12.5 percent had served for between 7-9 years. Another 9 or 28.8 percent of the respondents indicated to have served in the Police Force for between 10-12 years while 6 or 18.8 percent had served in the force for over thirteen years. The high number of officers who have served in the force over shorter periods of time can be explained by the high number of relatively new entrants being posted to CCU as compared to officers who have served longer in the force. This implies that most respondents have information about the cyber based financial crime and can be relied on in terms of sharing information on crime.

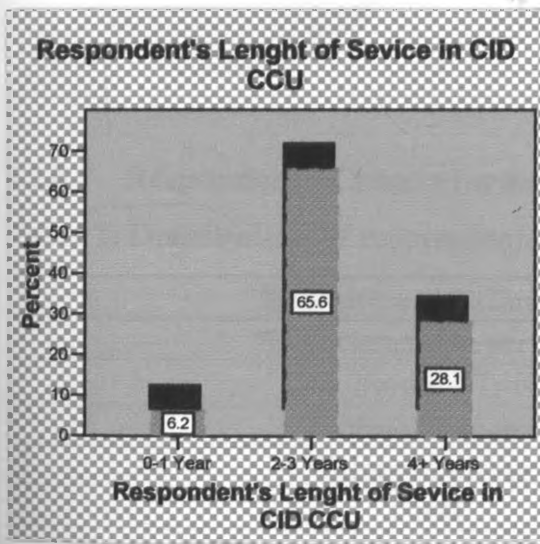
Figure 5: Respondents' Length of Service in the Police Force



4.2.6 Respondent's Length of Service in CID CCU

The majority of respondents (21 or 65.6 percent) were found to have served in the CID CCU for duration of between 2-3 years while 9 or 28.1 percent had served in the unit for more than four years. A minority (2 or 6.3 percent) had served in the unit for between 0-1 year. The large number of officers who had served at the unit for short durations as compared to the small number who had served in CID CCU for long periods could be explained by the relatively high turn over of officers at the unit due to transfers to other areas within the force or resignations from the force probably brought about by poor conditions of service such as low salaries.

Figure 6: Respondents' Length of Service in the CID CCU

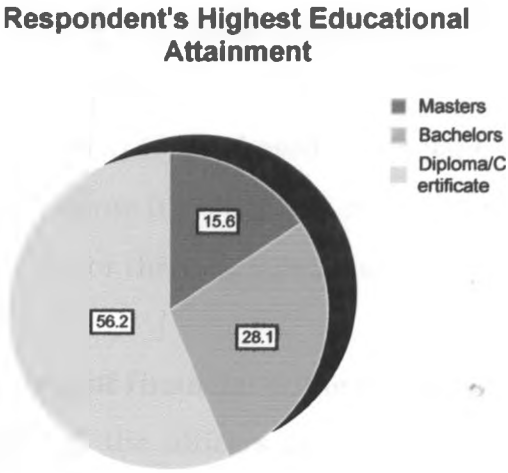


4.2.7 Respondent's Highest Educational Attainment

Figure 8 below shows that 18 or 56.3 percent of the respondents had attained either an academic diploma or certificate, 9 or 28.1 percent had bachelors degrees while 5 or 15.6 percent had had masters degrees. These results reveal that there are generally low levels of education reached by a majority of officers as a result

of low educational requirements at recruitment and subsequent low expectations by the force. As a result, majority of officers have not been required to pursue further education.

Figure 7: Distribution of respondents according to highest educational attainment



4.2.8 Respondent's Criteria for Recruitment

Table 1: Distribution of respondents according to criteria for recruitment to ccu

Recruitment Criteria	Frequency	Percent
Experienced in service	2	6.3
Qualified in IT/ICT	22	68.8
Normal transfer	5	15.6
Talent spotting	3	9.4
Total	32	100.0

The most important criterion for recruitment to CID CCU was found to be qualifications in IT or ICT which was represented by 22 or 68.8 of the respondents while the rest were recruited through normal transfer (5 or 15.6 percent), talent spotting (3 or 9.4 percent) and by experience gained (2 or 6.3 percent).

percent). These results show that recruitment process into CID CCU is well open to the fact that the role to be played by officers is special and therefore requires knowledge in IT or ICT. However, a few officers who find their way into the unit do so due to the age old culture of patronage where officers can be posted to any section of the force without adhering to their qualifications and subsequent capabilities to perform the specified tasks.

4.3 Findings and Analysis on Objective 1: Trends in Cyber based Financial Crime in Kenya

The Trends in Cyber based Financial Crime in Kenya are explained by cases of financial crime investigated, number of cases that occurred in the past one year, six months or three months, and the cases that were solved or not solved.

4.3.1 Cases of financial crime investigated

Majority of the officers at CID CCU (37.5 percent) investigated the group of financial crimes which consisted of Electronic Fraud, Pay roll Fraud, Identity Fraud and Card Fraud while 18.8 percent investigated cases of Obtaining by false pretences. Internet Scams and the group of crimes containing Threats, Extortions, Kidnappings and Human Trafficking were each investigated by 15.6 percent of the officers. Money Laundering was the crime which was investigated by the least number of officers at 12.5 percent. The first group of crimes containing Electronic Fraud, Pay roll Fraud, Identity Fraud and Card Fraud is the most investigated since it is also the most occurring in financial institutions. These crimes are more direct and enable fraudsters to steal money without presenting themselves at the financial institution and therefore present the least risk to the criminals. Another reason why these crimes are investigated by the larger number of officers is because the officers have the ability to do so and receive assistance from financial institutions which are interested in recovering the stolen proceeds.

Crimes of obtaining by false pretences also attract many criminals because they offer much more rewards due to the greedy human nature exhibited by victims. These crimes can also be committed without the criminal presenting himself at the financial institution. Alternatively criminals who use this mode of crime may use other persons to collect the stolen money from financial institutions. Internet Scams and the group of crimes containing Threats, Extortions, Kidnappings and Human Trafficking are crimes that can also be conducted over cyber space but are more risky in terms of arrest for the criminal. They are also not investigated often due to the investigation challenges they pose such as difficulty in ascertaining the location of the criminal. Money Laundering is the least investigated crime due to the difficulty it attracts in investigation. This is because the crime is perpetrated often in more than one country by organized criminals with connections and resources to conceal the crime.

Table 2: Cases of Financial Crime investigated by Respondents since Posting

Cases of Financial Crime investigated	Frequency	Percent
Threats, Extortions, Kidnappings and Human Trafficking	5	15.6
E-Fraud, Pay roll Fraud, Identity Fraud and Card Fraud	12	37.5
Internet Scams	5	15.6
Obtaining by False Pretences	6	18.8
Money Laundering	4	12.5
Total	32	100.0

4.3.2 Number of cases that occurred in the past one year

Table 3 below shows that majority (43.8 percent) of the officers at CID CCU investigated either between 1- 15 cases or between 53-200 cases of financial based cyber crime in the past one year. Only 12.5 percent of the officers investigated between 15 and 52 cases of financial based cyber crime in the past one year. These results show that during the period of the past one year, there were three

groups of officers, those who did the bulk of the work, those who performed moderately and those who did very little work.

This grouping in performance can be attributed to the officers' abilities as evidenced by their educational backgrounds and training. The officers who have more education are able to tackle more cases while those with the least education take on much less number of cases. The group with moderate cases is mainly those in the supervisory ranks such as the inspectorate and NCOs who apart from conducting investigations, also overlook the rest of the officers' work.

Table 3: Respondents' recollection of the number of cases handled in the past one year

Number of cases in the past one year	Frequency	Percent
1-15 Cases	14	43.8
15-52 Cases	4	12.5
53-200 Cases	14	43.8
Total	32	100.0

4.3.3 Number of Cases handled in the past six months

Majority (62.5 percent) of the officers at CID CCU investigated between 4-10 cases of financial based cyber crime in the past six months while 28.1 percent of the officers investigated between 42-100 cases of financial based cyber crime over the same period. Another 9.4 percent of the officers dealt with between 11-41 cases over the past six months. It can be deduced that the high number of officers who said that few cases of cyber based financial crime occurred is because they occupy low ranks and therefore do not appreciate the current trends in cyber based financial crime.

Those officers who indicated that they investigated the greatest number of cases are those in supervisory positions and those that are enlightened on the trends of cyber crime due to their superior educational levels and are therefore aware of the actual numbers of cases that are investigated. The least number of officers who gave the case figures to be between 11- 41 cases are those officers that are neither under supervisory ranks nor have little appreciation of trends in cyber crime but however have limited information about the actual number of cases over the period of six months.

Table 4: Number of cases that occurred in the past six months

Number of cases in the past six months	Frequency	Percent
4-10 Cases	19	62.5
11-41 Cases	3	9.4
42-100 Cases	9	28.1
Total	32	100.0

4.3.4 Number of cases handled in the past three months

Majority (62.5 percent) of the officers at CID CCU investigated between 2-10 cases of financial based cyber crime in the past three months while 21.9 percent of the officers investigated between 11-30 cases of financial based cyber crime over the same period. The least number of the officers (15.6 percent) dealt with between 31-40 cases over the past three months. It can be deduced that the high number of officers who indicated that the least number of cases of cyber based financial crime occurred is because of occupying lower ranks and therefore do not appreciate the current trends in cyber based financial crime because they lacked this information.

The officers who gave the case figures to be between 11-30 cases are those officers that are neither under supervisory ranks nor have little appreciation of trends in cyber crime. These officers have some information about the actual number of cases over the period of three months. Those officers who indicated

that they investigated the greatest number of cases are those in supervisory positions and those that are enlightened on the trends of cyber crime due to their superior educational levels and are therefore aware of the actual numbers of cases that are investigated.

Table 5: Number of cases that handled in the past three months

Number of cases in the past three months	Frequency	Percent
2-10 Cases	20	62.5
11-30 Cases	7	21.9
31-40 Cases	5	15.6
Total	32	100.0

4.3.5 Types of cases of financial based cyber crime solved

Table 6 below reveals that majority of the respondents (40.6 percent) indicated that they managed to solve cases of Electronic fraud followed by cases of Obtaining by false pretences (31.3 percent) and threats (12.5 percent). Another 12.5 percent of respondents indicated that they were able to solve cases of fraudulent websites and only 3.1 percent managed to solve cases of pornography. Cases of electronic fraud were easier to solve because they left an audit trail which enabled investigators to trace the culprits. Cases of obtaining by false pretences were also successfully investigated due to victims being able to give accounts of what had transpired which led to arrest and prosecution of offenders. This is also true in cases of threats and fraudulent web sites but difficulty in investigation was encountered for cases of pornography due to secrecy by which the crime is conducted.

Table 6: Financial based crime cases solved

Types of cases solved	Frequency	Percent
Obtaining	10	31.3
Threats	4	12.5
E-Fraud	13	40.6
Pornography	1	3.1
Fraudulent Web Sites	4	12.5
Total	32	100.0

4.3.6: Types of cases of financial based crime not solved

Majority of respondents (31.3 percent) indicated that they were not able to solve cases of Money Laundering followed by E-Commerce cases and Fraudulent Web Sites (25.0 percent each) and Threats (12.5 percent). Only 6.3 percent of the officers indicated that they were not able to solve cases of Credit Card duplication. The failure to achieve success in investigating cases of money laundering and electronic commerce can be attributed to difficulty in receiving investigation assistance from other countries. The same can also be said of cases of electronic commerce and fraudulent web sites. Threats and cases of credit card duplication did not pose a major obstacle to investigators since most occurred locally and assistance was received from ISPs and financial institutions which made investigation easier.

Table 7: Financial based crime cases not solved

Types of cases not solved	Frequency	Percent
Threats	4	12.5
Fraudulent Web Sites	8	25.0
Money Laundering	10	31.3
E-Commerce Cases	8	25.0
Credit Card Duplication	2	6.3
Total	32	100.0

4.4 Findings and Analysis on Objective 2: Structures and Mechanisms for Cyber Policing and Crime Prevention in Financial Institutions in Kenya

This section lists the respondents' training prior and after posting to CCU, the responsibilities they are assigned in their current post and the mechanisms for cyber crime prevention in financial institutions.

4.4.1 Respondent's Training prior to posting to CCU

Table 8 below reveals that majority of respondents (13 or 40.6 percent) indicated that general police work was the type of training they received before joining CID CCU while 9 or 28.1 percent had computer academic qualifications. A further 6 or 18.8 of the respondents had received fraud training while 4 or 12.5 came in with instructions on basic cyber crime. It can be deduced that the large majority of respondents being police officers, had all received training in general police work. It can also be deduced that officers had interest in IT work and therefore sought prior training in computer technology on their accord. The minority who received training in either fraud training or cyber crime were the exception rather than the norm since few courses are usually offered by the department in these two areas. A strong incentive for officers to join CID CCU therefore is to receive training in cyber crime, fraud and other IT areas.

Table 8: Training prior to posting to CCU

Training before Posting	Frequency	Percent
Computer academic Qualifications	9	28.1
General Police Work	13	40.6
Basic Cyber Crime Investigations	4	12.5
Fraud Training	6	18.8
Total	32	100.0

4.4.2 Training after posting to CCU

In-house training on Computer and Cellular forensics was the most common type of training received by respondents (10 or 10.3 percent), followed by cyber crime courses represented by 9 or 28.1 of the respondents and ISDE (7 or 21.9 percent). Only 3 or 9.4 percent of respondents ENCASE and FTK forensic tool kits training was received by 3 or 9.4 percent of respondents while 2 or 6.3 percent of the respondents received training in proactive internet investigations.

Only 1 or 3.1 percent of the respondents had received Training the Trainer course after joining CID CCU. These results show that training at CID CCU mainly concentrates on the first three courses namely In-house training on Computer and Cellular forensics, cyber crime and ISDE because the courses address the core mandate of the unit and therefore are designed to equip the officers with skills to tackle their duties. These courses are also cheaper and convenient to offer since local resource persons are able to provide them at shorter periods of time. The rest of the courses namely ENCASE and FTK forensic tool kits training, proactive internet investigations and Training the Trainer course are either offered by personnel brought in with the assistance of foreign countries, are relatively expensive or do not address the core mandate of CID CCU directly.

Table 9: Training after posting to CCU

Training after posting	Frequency	Percent
ENCASE and FTK Forensic Tool Kits	3	9.4
In-house Training on Computer and Cellular Forensics	10	31.3
Training of Trainer Course	1	3.1
Identification and Seizure of Digital Evidence	7	21.9
Cyber Crime Courses	9	28.1
Proactive Internet Investigations	2	6.3
Total	32	100.0

4.4.3 Responsibilities assigned in current post

Majority of the officers at CID CCU (34.4 percent) indicated that they mainly performed cyber crime Investigations, 28.1 percent said that they did computer and cellular forensics at the unit while a similar number (28.1 percent) revealed that they engaged in ISDE and examining for other Police Departments. A small number represented by 6.3 percent did awareness training to Government agencies and to colleagues while 3.1 percent performed other investigations not related to IT. These results show that though officers considered themselves as professionals tasked with core investigations in cyber crime, computer and cellular forensics and ISDE, poor management resulted in some of them being given duties that are either not related to IT or task them with training other officers in the force, a job which outside the mandate of CID CCU.

Table 10: Responsibilities assigned in current post

Responsibilities assigned in current post	Frequency	Percent
Cyber Crime Investigations	11	34.4
Computer and Cellular Forensics	9	28.1
Other investigations not related to IT		
ISDE and examining for other Police Departments	9	28.1
Awareness training to Government agencies and Colleagues	2	6.3
Total	32	100.0

4.4.4 Mechanisms for cyber crime prevention in financial institutions

Majority of the respondents (40.6 percent) indicated that liaisons and intelligence sharing was key in cyber crime prevention while 28.1 percent selected updated IT infrastructure. Enhanced legislation was selected by 18.8 percent of the respondents while training of stakeholders was chosen by 12.5 percent of the respondents. Since criminals move from one financial institution to the next, sharing of information on a regular basis will go a long way towards informing

authorities about the crime trends and the criminals' modus operandi. This will assist in setting up adequate protection measures that will prevent more cyber crimes.

Establishment of robust IT departments, enhancement of access controls, system audits and implementation of management systems will go a long way towards preventing cyber crimes. Enhanced legislation to regulate the industry and curb cyber crime through punishment and deterrence will also contribute towards prevention of cyber crime. The same thing can also be said about training of stakeholders which will raise awareness and therefore enable them to detect and prevent cyber crime proactively.

Table 11: Mechanisms for cyber crime prevention in financial institutions

Mechanisms for cyber crime policing and prevention	Frequency	Percent
Liaisons and Intelligence sharing	13	40.6
Updated IT infrastructure	9	28.1
Training of stakeholders	4	12.5
Enhanced legislation	6	18.8
Total	32	100.0

4.5 Findings and Analysis on Objective 3: Obstacles to the prevention of Cyber based financial crime in Kenya

This section deals with the respondents' reasons for not solving cyber based financial crime cases, liaisons established to support the respondents' work, liaisons not established but important to support the work and how deployment practices support the respondents' work. The section will also look at how deployment practices do not support the respondents' work.

4.5.1: Reasons for not solving cases

The most cited reason given by 53.1 percent of the officers for not being able to solve cases of financial based cyber crime was the lack of transboundary cooperation followed by legal and investigations drawbacks which was chosen by 34.4 percent of the officers. Lack of cooperation by ISPs was selected by 6.3 percent of the respondents while political interference and lack of software equipment were each chosen by 3.1 percent of the officers. Most of the cyber based financial crime cases that the officers were not able to solve were those of money laundering, electronic commerce and fraudulent web sites which often took place over more than one country. Lack of cooperation between states where these crimes were perpetrated therefore presented the greatest obstacle to resolving these cases.

Legal and investigations drawbacks also offered a challenge since investigations required thorough knowledge and skills on cyber based financial crimes while prosecution depended on better legislation. The scenario at the moment is that most officers inside and outside the CID CCU do not have up-to-date skills on investigation of cyber based financial crime while the court system still depend on laws which are ineffective against cyber financial crimes. Lack of cooperation by some ISPs affected successful investigations since the CID CCU relied on information from ISPs. Political interference also accused a drawback to the fight against cyber based financial crime since failure by government to give reasonable priority to this issue has resulted to proliferation of these crimes. The same can be said of the lack of software equipment due to insufficient resource allocation which has therefore handicapped investigations.

Table 12: Respondents' reasons for not solving cases

Reasons for not solving cases	Frequency	Percent
Lack of transboundary cooperation	17	53.1
Lack of cooperation by ISPs	2	6.3
Political interference	1	3.1
Lack of software and equipment	1	3.1
Legal and investigations drawbacks	11	34.4
Total	32	100.0

4.5.2: Liaisons established to support work

Table 13 below shows that majority of the respondents (31.3 percent) regarded the liaisons between CID CCU and other government departments and bodies as the most effective followed by ISPs (28.1 percent). The liaisons between CID CCU and foreign embassies were chosen by 21.9 percent of the respondents while that of Interpol was 18.8 percent. It can be deduced that cooperation with other government departments and bodies is excellent given that there is no red tape involved while ISPs have been of assistance due to the regulatory role played by CCK which has ensured that ISPs comply and assist CID CCU appropriately.

Foreign embassies offer training and information about cyber based financial crime to CCU but play a limited role in tracking suspects wanted by CCU in their countries. The same can also be said about Interpol which also provides information but offer limited investigation assistance to CID CCU due to legal drawbacks. Despite the existence of the effective liasons above, those with banks are still lacking in effectiveness.

Table 13: Awareness of the liaisons established to support work

Liaisons established to support work	Frequency	Percent
Interpol	6	18.8
Foreign Embassies	7	21.9
ISPs	9	28.1
Govt Depts. and bodies	10	31.3
Total	32	100.0

4.5.3: Liaisons not established but important to support work

Majority of the officers at CID CCU (37.5 percent) indicated that direct connection between ISPs and CCU server was the liaison that was most required followed by communication network with the outside world (18.8 percent) and training of other law enforcers on cyber crime (18.8 percent). Banks and Cyber Cafes were each chosen by 12.5 percent of the respondents as the liaisons not established but important to support work. It can be deduced from these results that direct interaction with ISPs and the outside will reduce the time taken to complete investigations due to ready availability of information. The time wasted in seeking information from ISPs and other countries will therefore be eliminated and the result will be faster investigations, apprehension and prosecution of suspects.

The liaison with banks has also been missing despite its importance given that information on cyber based financial crimes mostly emanates from banks and other financial institutions. Banks have also not been willing to reveal these cases for fear of painting a negative picture to their customers and thereby losing business. The liaisons with cyber cafes are also important for purposes of solving cases of threats, fraudulent web sites, pornography and electronic fraud. However these have not been established due to the absence of policies.

Table 14: Respondents' views on the liaisons not established but important to support work

Liaisons not established	Frequency	Percent
Cyber Cafes	4	12.5
Direct connection between ISPs and CCU Server	12	37.5
Training of other Law Enforcers on Cyber Crime	6	18.8
Communication Network with Outside World	6	18.8
Banks	4	12.5
Total	32	100.0

4.5.4: How deployment practices support work

Table 15 below indicates that 46.9 percent of the officers at CID CCU revealed that the current deployment practices supported their mandate through specialization which enhances efficiency and personal fulfillment of the officers. Similarly, posting of qualified staff due to merit was chosen by 31.3 percent of the respondents followed by provision of short term courses (12.5 percent). Only 9.4 percent of the respondents indicated that the current deployment practices at CID CCU did not play any role in supporting their work. It can be deduced that encouraging specialization enhances efficiency and personal fulfillment which translates into better performance by the unit. This ensures that the unit addresses its mandate effectively. The same thing can also be said about posting of qualified staff due to merit which ensures that CI CCU is made up of competent personnel to be relied on to conduct successful investigation and aid prosecution of cyber based financial crimes.

Provision of short term courses is also critical in aiding the ability of CCU officers to investigate cases. This is in view of the fact that technology changes rapidly while criminals become more and more sophisticated. In order to be relevant and achieve their mandate, officers must continuously update themselves on the

current trends of cyber based financial crime. The minimal choice that the current deployment practices at CID CCU did not play any role in supporting the officers' work can be attributed to the few officers in possession of university degrees. These officers regard the unit as still made up of unqualified personnel who pose an obstacle to effective investigation of cyber based financial crimes.

Table 15: Respondents' views on how deployment practices support work

How deployment practices support work	Frequency	Percent
Posting of qualified staff due to merit	10	31.3
Specialization enhances efficiency and fulfillment	15	46.9
Provision of short term courses	4	12.5
No Supporting Role	3	9.4
Total	32	100.0

4.5.5: How deployment practices do not support work

Majority of the officers (40.6 percent) indicated that deployment practices at CID CCU were a drawback to their work by facilitating misplaced deployments. That transfers cause brain drain or loss of skills was chosen by 25.0 percent of the officers while outside the drawback that external training affects staff efficiency was chosen by 18.8 percent of the officers. Deployment practices did not also support the officers' work as evidenced by the management that was not well versed in cyber crime (12.5 percent) and inadequate remuneration (3.1 percent).

Misplaced deployments cause the wrong officers to be taken out and into the unit thereby causing challenges in investigation. When officers who possess superior qualifications in IT and ICT are replaced by those with inferior or without any qualifications in IT and ICT, the results are poor investigations. This can also be said of transfers which ultimately cause brain drain or loss of skills since officers who have worked at the unit for some time gain invaluable experience which can only be utilized at the same unit. Due to the limited number of officers at CID CCU and the corresponding high trends of cyber

crimes, the unit is overstretched. External training will therefore remove officers from their work station and this will cause a further strain on the ability of the unit to meet its mandate.

Due to staffing challenges as that posed by the lack of senior officers who are qualified in IT and ICT, the officer in charge of CID CCU does not possess qualifications in IT and ICT. Most of the senior officers in CID and the Police force are also not well versed in cyber crime and this poses a challenge in policy making and direction of operations at the unit. As a result, good policies are not formulated and resources are not directed to support the role of the unit since top management does not appreciate the trends of cyber crime. Only one officer indicated that inadequate remuneration was an issue though this is a grievance held by many within and without the unit. Considering that personnel possessing the same levels of qualifications in the private sector earn much more than their peers at CID CCU, this is bound to be a contentious issue. This is because issues of agitating openly for better remuneration within the Police Force are taboo subjects which can result in dismissal or punishment and therefore are placed in the back seat.

Table 16: Respondents' views on how deployment practices do not support work

Deployment practices that do not support work	Frequency	Percent
Arbitrary transfers cause Brain drain/ Loss of Skills	8	25.0
affects Staff Efficiency	6	18.8
Misdeployments	13	40.6
Management not well versed in Cyber Crime	4	12.5
Inadequate Remuneration	1	3.1
Total	32	100.0

4.6 Findings and Analysis on Objective 4: Capacity of CID CCU in preventing Cyber based Financial Crimes in Kenya

This section deals with capacity of CID CCU in preventing cyber based financial crimes and will look into ways of addressing limitations in operations, the resources required to function effectively and the resources that are adequately supplied. The section also discusses the resources not adequately supplied, the causes of deficiency in supply of resources and the contribution of respondents to ensure their own preparedness.

4.6.1 Ways of addressing limitations in operations

Table 17 below shows that most of the officers (28.1 percent) chose continuous and localized training as the best way of addressing limitations in operations at the CID CCU. Enhancing funding for equipment, software and remuneration was chosen by 21.9 percent of the officers while placement of qualified management was the choice of 15.6 percent of the officers. Recruiting and retaining qualified officers was chosen by 12.5 percent of the officers, enhancing legislation and policy making by another 12.5 percent of the officers while correct placement and specialization was the choice of only 9.4 percent of the officers.

These results reveal that continuous and localized training will address possession of skills which is one of the most critical limitations facing the unit. In turn this will facilitate superior performance of officers in investigation and prevention while the end result will be successful prosecution and a general decline of cyber crime cases by imparting awareness to potential victims. Enhancing funding for equipment, software and remuneration will also address another important challenge facing the unit since this will also facilitate better performance by the officers in fulfilling the mandate of the unit. Placement of qualified management will ensure that top level decisions are made in view of

requirements of the unit and this will lead to the unit receiving the needed resources through sufficient budgetary allocations.

Recruiting and retaining qualified officers will ensure that officers posted to the unit are an asset and not a liability to the unit. This is because such officers will have the ability to successfully investigate cases of cyber crime and build on this knowledge over time. The unit will also benefit because such officers are easier to train further and have interest in their work by virtue of their specialized expertise. The same will also apply in the correct placement and specialization of the officers in the unit since they will focus on one area that is cyber crime. The results will be prevention, effective investigation and prosecution of cyber crimes which will eventually lead to reduced cases of cyber crimes.

Table 17: Respondents’ suggestions on addressing limitations in operations

Ways of addressing limitations in operations	Frequency	Percent
Recruit and retain qualified officers	4	12.5
Adequate funding for equipment, software and remuneration	7	21.9
Continuous contextualized training	9	28.1
Qualified(cyber trained) management	5	15.6
Correct placement and specialization	3	9.4
Enhance legislation and policy making	4	12.5
Total	32	100.0

4.6.2 Resources required by Respondents to function effectively in the unit

The table below shows that majority of respondents (31.3 percent) cited forensic tools and consumables as the resources that they required to function effectively, closely followed by licenses and updates for software (28.1 percent) and continuous training and certification (25 percent). Only 15.6 percent of the respondents said that they required transport and communications in order to function effectively in their positions. It can be deduced from these results that

items that addressed the mandate of the unit directly attracted the most demand since they were vital for the day to day running of operations at CID CCU. These items include tools used in forensic investigations, consumables such as storage devices like USB discs and computers. Licenses and updates for software is also key in the operations of the unit just as continuous training and certification. The former enable officers to be able to freely utilize software in facilitating their work while the later give the officers current skills, knowledge and recognition to apply expertise in their duties.

Table 18: Resources required to function effectively in the position

Resources required	Frequency	Percent
Continuous Training and Certification	8	25.0
Transport and Communications	5	15.6
Forensic Tools and Consumables	10	31.3
Licenses and Updates for Software	9	28.1
Total	32	100.0

4.6.3 Adequately supplied resources

The results of table 18 below reveal that majority of the respondents (56.3 percent) indicated that none of the resources that they required to function effectively in their position were adequately supplied or provided while 21.9 percent identified forensic tool kits as the resources that were supplied. 9.4 percent of the respondents revealed that they received institutional support while only 6.3 percent each indicated that internet connectivity and training was provided. These results show that CID CCU is not well prepared in terms of supply of resources to meet their mandate.

Table 19: Respondents' views on resources that are adequately supplied

Resources adequately supplied	Frequency	Percent
None	18	56.3
Internet Connectivity	2	6.3
Training	2	6.3
Forensic Tool kits	7	21.9
Institutional Support	3	9.4
Total	32	100.0

4.6.4 Resources that are not adequately supplied

A majority of the respondents (40.6 percent) revealed that all resources were not adequately supplied at the unit while 31.3 percent of the respondents said that transport and forensic tools were not adequately supplied. Out of all the respondents, 15.6 percent of the respondents said that qualified personnel were in short supply in the unit while only 12.5 percent identified training as not provided at the unit. These results show that the unit is generally not adequately supplied with the key resources in order to achieve its mandate. This might be due to the CID department and the Police force in extension not regarding cyber crime as an important crime and CCU as a vital investigative arm.

Table 20: Resources that are not adequately supplied

Resources not Adequately Supplied	Frequency	Percent
All	13	40.6
Qualified personnel	5	15.6
Training	4	12.5
Transport and Forensic Tools	10	31.3
Total	32	100.0

4.6.5 Causes of deficiency in supply of resources

The table below indicates that majority of the respondents (37.5 percent) attributed lack of resources at CID CCU to an inadequate budget while 31.3

percent laid the blame on low understanding of cyber crime and poor ICT policy. Only 15.6 percent of the respondents said that the cause of deficiency in resources was lack of qualified leadership and personnel while a similar number pointed to poor training as the cause. It can be deduced that government has not prioritized the fight against cyber crime by not allocating sufficient funds to the unit. Vital resources required at CID CCU have not been supplied and as a result prevention of cyber based financial crime has been compromised.

Table 21: Causes of deficiency in supply of resources

Causes of deficiency	Frequency	Percent
Low understanding of Cyber Crime and Poor ICT Policy	10	31.3
Inadequate Budget	12	37.5
Lack of Qualified leadership and Personnel	5	15.6
Poor Training	5	15.6
Total	32	100.0

4.6.6 Action to ensure own preparedness for the role

Early preparation of incidence tools and personal efforts were the most selected actions (31.3 percent each) to ensure preparedness for roles by the respondents. Almost 22 percent of the respondents (21.9 percent) chose continuous reading and consulting as the way they prepared for their role at the CID CCU while 15.6 percent of the respondents made work plans to ensure their own preparedness for the duties at the unit. It can be deduced that since IT work requires incidence tools, officers at the unit have no choice but to use these equipments in their daily duties. Similarly, since it is necessary to utilize consumables such as storage devices like USB disks, officers take it upon themselves to purchase these items in order to be able to carry on with their duties though not to their complete satisfaction.

Continuous reading, consulting and work plans were the least chosen ways because of the general low levels of higher education among the officers. This occurs for the reason that persons with low levels of education do not appreciate to develop and improve their skills and knowledge through reading, learning and making plans for the work they intend to do. The result is that most officers at CID CCU do not look beyond what they are doing and as a result do not learn new trends of cyber crime investigations which affects the overall ability of the unit to meet their prevention and investigation mandates.

Table 22: Respondent's action to ensure own preparedness for the role

Action to ensure own preparedness	Frequency	Percent
Continuous reading and Consulting	7	21.9
Work Plan	5	15.6
Early Preparation of Incidence Tools	10	31.3
Personal Efforts	10	31.3
Total	32	100.0

CHAPTER FIVE

SUMMARY OF FINDINGS, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This section provided for findings made, recommendations and conclusions and areas that needed further research. The recommendations focused on the thematic areas of study namely trends in cyber based financial crime, structures and mechanisms of cyber policing and crime prevention in financial institutions in Kenya, obstacles to prevention of cyber based financial crimes and capacity of CID CCU in preventing cyber based financial crimes in Kenya.

5.2 Summary of Findings

The findings were made in light of objectives of the study and they show that the most investigated cases of financial crime at CCU were the group of financial crimes consisting of electronic fraud, pay roll fraud, identity fraud and card fraud. On the number of cases investigated at CCU, it was found that between 1-15 cases were investigated in the past one year, between 4-10 cases in the past six months and between 2-10 cases in the past three months. These results indicated that financial institutions did not report cases to CCU despite the high trends of cyber based financial crimes they experienced. This is mainly due to the perception of CCU's limited ability and the fear of business/client loss and bad publicity among financial institutions. It was also found that majority of the respondents were able to solve cases of electronic fraud but were unable to successfully solve those of money laundering.

Many of the officers at CCU had attained either an academic diploma or certificate showing that there are generally low levels of education reached by the officers. Consequently, the most common criteria for recruitment to CID CCU was qualification in IT or ICT which was mainly a diploma or a certificate. However, there are a few cases where a few officers are posted to the unit due to

patronage. It was found that general police work was the most common type of training received by officers before joining CID CCU which indicated low levels of technical knowledge on cyber policing. In-house training on computer and cellular forensics was the most common type of training received by the officers after joining the unit because it addressed the core mandate of the unit and is also cheaper and convenient to offer. The main duty of officers posted to the unit is cyber crime investigations. On mechanisms for cyber crime prevention in financial institutions, it was found that financial institutions advocated for liaisons and intelligence sharing among stakeholders, enhanced legislation, updated IT infrastructure and training of stakeholders.

Most officers at CID CCU had served in the Police Force for short periods of time because of the many new entrants being posted to CCU as compared to officers who have served longer in the force. The same is also true for the length of service at CID CCU which was shorter because of the high turn over of officers at the unit due to transfers to other areas within the force or resignations from the force probably brought about by poor conditions of service. This impacts negatively on the performance of the officers and of the unit since skilled and experienced personnel are constantly lost. The reason that was given for the inability to solve cases of money laundering was lack of transboundary cooperation and legal and investigations drawbacks. This entails absence of cooperation between states and inadequate skills among officers at the CCU.

On liaisons established to support their duties at CCU, most officers said that the liaisons between CID CCU and other government departments were strongest. However those between CCU and financial institutions were considerably lower an indication of poor relationship. The officers also wished most for stronger liaisons between CCU and ISPs through a direct connection in the servers. Though the officers also wished for liaisons with banks, it was obvious that CCU

has not received any cyber based financial crime cases from banks lately. This is because banks have not been willing to report these cases for fear of losing business and instead report some of these cases to BFID. It was found that majority of the officers supported the current deployment practices at CCU for reasons of encouraging specialization for efficiency and the officers' personal fulfillment. However, the officers criticized the same deployment practices at CID CCU due to facilitating misplaced deployments which brought in unqualified officers and took away skilled and experienced officers.

It was found that in order to address limitations in operations at CCU, continuous and localized training, and sufficient budgetary allocations were to be given priority. It was also found that a majority of the respondents required forensic tools and consumables in order for them to function effectively. However, none of the resources that were required were adequately supplied which is one of the leading causes of below par performance by the unit. The most common reason given for this lack of adequate supply of resources is inadequate budgetary allocation by the government, low understanding of cyber crime and poor ICT policy. Majority of the respondents prepared their incidence tools early and put in personal efforts in order to conduct effective cyber crime investigations. These efforts included purchasing consumables like storage devices such as USB disks.

5.3 Conclusion

From the above findings, conclusions can be drawn that the high turn over of officers at the unit due to transfers to other areas within the force and or resignations impacts negatively on the capacity of CID CCU. Inadequate supply of the required resources due to inadequate budgetary allocation has also resulted in low capacity of the CID CCU. The CCU has investigated very few cases of financial based crimes because financial institutions have not recognized

their mandate since CCU has weak capacity to investigate these cases successfully. It can be concluded that the liaisons between CCU and financial institutions are visibly missing. CCU was only able to solve very few cases of electronic fraud and this could be regarded as a reflection of low capacity of the CCU in cyber crime prevention.

The deployment practices at CID CCU facilitate misplaced deployments by bringing in mismatched roles and skills and taking away skilled and experienced officers. In order to address limitations in operations at CCU, continuous local and international training and sufficient budgetary allocations was identified as key and therefore deserved to be given priority. The CID CCU therefore lacks the capacity to prevent cyber based financial crimes in Kenya.

5.4 Recommendations

5.4.1 Policy Recommendations

The government should ensure that the available legal instruments are regularly reviewed. Financial based Cyber crimes should be prosecuted under Penal Code Act and acts such as the Kenya Communications Act of 1998, Kenya Communications Amendment Act No. 1 of 2008 and the Crime and Money Laundering Act of 2009..

The government should also sensitize and educate law enforcement agencies, the public and financial institutions on the importance of protection against cyber

Adequate budgetary allocations, proper deployment practices and stronger liaisons especially with financial institutions will enhance the units' capacity in cyber crime prevention.

The government should work with other countries by establishing mutual legal agreements and stronger financial cyber crime legislation.

Implementation of the Ransley report will be key and will include decentralization of the police establishment to encourage professionalism, enactment of the Police Reforms Act to implement reforms and the creation of the Police Reforms Implementation Commission to institutionalize the reforms, Other recommendations include establishment of a Police Service Commission and the implementation of a National Policing Policy and a National Security Policy.

The CID CCU should be broadened and decentralized with technical, competent and with high ranked leadership probably at the level of a Senior Assistant Commissioner of Police (S/ACP).The CCU should be staffed with more and adequate personnel.

5.4.2 Recommendations for Further Research

This study focused on assessing the CID CCU in preventing cyber based financial crime in Kenya. It was noted that this matter has not been given due attention by the government and other stakeholders. Further studies are therefore recommended in other sectors in Kenya such as in communication and finance to get a true picture of the problem and to promote strategies which can tackle the problem economically and efficiently.

REFERENCES

- ACFE (2006), *Fraud Detection, Report to the Nation*. London: ACFE
- Ajala, E.B. (2007), *Cybercafés, Cyber Crime Detection and Prevention*. Library Hi Tech News. No.7. Pp. 26-29. Emerald Group Publishing Ltd.
- Armstrong, H.L. and Forde P.J. (2008), *Internet Anonymity Practices in Computer Crime*. Information Management and Computer Security 11/5. Pp. 209-215.
- Babbie, E. (1995), *The Practice of Social Research*, 7th Edition Boston: Wadsworth Publishing Company.
- Bernard, H.R. (1995), *Research Methods in Anthropology: Qualitative and Quantitative Approaches*, 2nd Edition, London: Altamira Press.
- Bower, B (1988), *Chaotic Connections*, Science News (Jan. 1988): 58-59.
- Brewer, J. and Hunter, A. (1989), *Multimethod' Research: A Synthesis of Styles*: London: Sage Publications.
- Burns P. and Stanley A. (2002), *Fraud Management in the Credit Card Industry*, Discussion Paper presented in a Seminar at Payment Card Centre of the Federal Reserve Bank of Philadelphia, April 2002, Philadelphia USA. Available from <http://www.philadelphia.org>
- Camner B. (1972), *Credit Card Fraud: The Neglected Crime*, The Journal of Criminal Law and Criminology 76 (3) 102-125
- CBK (2005), *Risk Management Survey Report*. CBK

- CBK (2008), *Bank Supervision Annual Report 2008*. CBK. Available at <http://www.centralbank.go.ke>
- CCK (2006), *National ICT Policy. January, 2006*. CCK
- CCK(2009), *Sector Statistics. April-June, 2009*. CCK
- Computer Science and Telecoms Board (CSTB) (2001), *Cyber Security and the Insider Threat to Classified Information: Summary Discussions at a Planning Meeting on Critical Infrastructure Assurance Meeting (CSTB)*.
- CSFI(2010), *Banking on Banana Skins. The CSFI Survey of Bank Risk*, CSFI
- De Groot, A.D. (1969), *Methodology: Foundations of Inference and Research in the behavioural Sciences*. The Hague: Mouton.
- Delbaso, M. and Lewis, A.D. (2001), *First Steps: A Guide to Social Research Ontario*: Nelson
- Denzin, N.K. and Lincoln Y.S. (2003), *Strategies of Qualitative Inquiry* London: Sage Publications.
- Dombrowski, S.C., Gischlar, K.L. and Durst, T. (2007), *Safeguarding Young People from Cyber Pornography and Cyber Sexual Exploitation: A Major Dilemma of the Internet*, *Child Abuse Review* 16 (1), 153 - 170.
- Dutta, A. and Roy, R. (2008), *Dynamics of Organized Information Security*, *System Dynamics Review*, 24(3), pp. 349-375.

Fletcher, N. (2007), *Challenges for Regulating Financial Fraud in Cyber Space*. Journal of Financial Crime 14 (2). Pp. 190-207. Emerald Group Publishing Ltd.

Garcia G. (1980), *Credit Card: an Interdisciplinary Survey*, Journal of Consumer Research 6(4), 14-21.

Giddens, A. (1991), *The Consequences of Modernity*: California: Policy Press Cambridge.

Grabosky, P and Smith, R. (1998), *Crime in the Digital Age*. Federation Press and Australian Institute of Criminology. Sydney.

Grant, A.E. and Meadows, J.H. ed (2002), *Communication Technology Update*, 8th Edition. Oxford: Focal Press

Granville. J. (2003), *Dot.Com; The Dangers of Cyber Crime and a Call for Proactive Solutions*. Australian Journal of Politics and History. 49 (1). Pp. 102-109.

Hoy, D.C. and Mc Carthy, T. (1994), *Critical Theory*. Cambridge: Blackwell Publishers

Hoyle, R.H. et al (2002), *Research Methods in Social Relations* Melbourne: Wadsworth.

Huberman, A.M. and Miles, M.B. (2002), *The Qualitative Researcher's Companion*, London: Sage Publications.

ICTJ (2010), *Security Sector Reform and Transitional Justice in Kenya*. International Center for Transitional Justice.

- Kasidi, J. (2009), "Cheques Payments for Over 1 Million Stopped." Daily Nation, 1st October 2009.
- Kidder, L.H. and Judd, C.M. (1986), *Research Methods in Social Relations*, 5th edition New York: CBS Publishing Japan Ltd.
- Kothari, C.R. (2004), *Research Methodology: Methods and Techniques* New Delhi: Kings Mill.
- Kumar, R. (2005), *Research Methodology: A Step By Step Guide For Beginners*, 2nd edition New Delhi: Sage Publications.
- Kovacs, D.K.(1995), *Internet Trainers Guide*. New York: Van Nostrand Reinold
- Langenderfer, J. and Shimp, T.A.(2001), *Consumer vulnerability to Scams, Swindles and Fraud: A New Theory of Visceral Influences on Persuasion*. *Psychology and Marketing*, 18(7), pp. 763-783.
- Levi M. (2006), *Risk and Crime: Shifting Moral Boundaries: The Media Construction of Financial White Collar Crimes*, *British Journal of Criminology* 46(6) 1037-1056.
- Maffly D. and McDonald A. (1960), *The Tripartite Credit Card Transaction: A Legal Infant*, *California Law Review* 48 (3) 93-117.
- Marron D. (2007), *Alter reality' Governing the Risk of Identity Theft*, *British Journal of Criminology* 13(2) 85-117.
- Mason, J. (2004) *Qualitative Researching*, 2nd Edition, London: Sage

Masuda B. (1992), *Credit Card Fraud Prevention: A Successful Retail Strategy*, Security Management 36: 71-74

Mc Crohan, K.F. (2003), *Facing the Threats to Electronic Commerce*. Journal of Business and Industrial Marketing 18 (2) Pp. 133-145.

Neuman, L.W. (1994), *Social Research Methods: Qualitative and Quantitative Approaches*, 2nd edition Boston: Allyn and Bacon.

OECD (2008), *Economic, Environmental and Social Statistics*, OECD Fact book, OECD.

OECD (2001), *Cross-border Co-operation in Combating Cross-border Fraud: The US/ Canadian Experience*. OECD Digital Economy Papers No. 65, OECD

OECD (2009), *Cyber Security and Economic Incentives*, Science and Information Security. OECD, (2), 105-118

Overill, R.E. (2003), *Reacting to Cyber-Intrusions*. The Technical, Legal and Ethical Dimensions. Journal of Financial Crime 11 (2). Pp. 163-167.

Pant, H. (2006), *Optimal Availability and Security for IMS – Based Voip Networks*. Bell Labs Technical Journal II (3), 211-223. Wiley Periodicals.

Parsons, T. (1979) *The Social Systems* London: Routledge and Kegan Paul.

PwC (2009) *Economic Crime in a Downturn*. Global Economic Crime Survey. London: FSRI

- Ritzer, G. (1992) *Sociological Theory*. New York: MC GrawHill.
- Salifu, A. (2008), *The Impact of Internet Crime on Development*. *Journal of Financial Crime*, 15 (4) Pp. 432-443.
- Sliter, J. (2006), *Organized Crime in Business*. *Journal of Financial Crime*, 13(4). Pp. 383 - 386.
- Snyder, H and Crescenzi, A (2009), *Intellectual Capital and Economic Espionage. New Crimes and New Protections*. *Journal of Financial Crime*, 16 (3). Pp. 245-254.
- UNODC (2007a), *First Meeting of the Core Group of Experts on Identity -Related Crime*. Courmayeur Mont Blanc, Italy. 29-30 November 2007. Commission on Crime Prevention and Criminal Justice.
- UNODC (2007b), *First Meeting of the Core Group of Experts on Identity -Related Crime*. Vienna, Austria. 6-8 December, 2010. Commission on Crime Prevention and Criminal Justice.
- Verfaillie, K and Vander Beken, T. (2008), *Proactive Policing and the Assessment of Organized Crime*. *Policing: An International Journal of Police Strategies and Management*. 31(4). Pp. 534-552.
- Wallis, W.A. and Roberts, H.V. (1956), *The Nature of Statistics*. New York: The Free Press.
- Wilson, E.J. (2005), *What is internet governance and where does it come from ?* *Journal of Public Policy*, Pp. 29 - 50

Wright, A. (2002), *The Changing Competitive Landscape of Retail Banking in the E-Commerce Age*. Thunderbird International Business Review, 44(1). Pp 71-84.

Magazines

Aron, M. (2010), "*Kenyan Banks lose Sh. 1.7 billion to fraudsters in 3 months*". The Standard, 9th November, 2010. Pp.14

Daily Nation Correspondent (2009), "*Officers receive Cyber Crime Training*." Daily Nation 3rd January, 2009. Pp. 24

Daily Nation Correspondent (2010), "*Kenyan detectives found wanting*". Daily Nation 7th July, 2010. Pp.18

Business Daily Correspondent (2010a), "*Cyber Security Boosts Demand for Software*". Business Daily, 13th September, 2010. Pg. 7.

Business Daily Correspondent (2010b) "*Kenyan banks are losing Sh. 1.7 billion in 3 months*", Business Daily, 25th November, 2010.

Kinyanjui, K. (2010), "*Kenya tops List of East Africa Countries Worst-hit by Computer Viruses*". Business Daily. Thursday September 9, 2010. Pp. 8.

Njuguna, N. and Etemesi, R. (2010), "*How Local Banks are Coping with fraud*". Daily Nation, 10th August, 2010. Pp. 26.

Okoth, J. (2009), "*Fraudsters take home billions from banks*". Nairobi: East Africa Standard 17th November.

Electronic Sources

CBK (2003), *CBK Payments System in Kenya*, September, 2003 from <http://www.centralbank.go.ke>

CBK (2008), From [www.centralbank.go.ke/financialsystem/credit reference/](http://www.centralbank.go.ke/financialsystem/creditreference/) Introduction

CBK (2010a), *Kenya Monthly Economic Review*, August 2010 from <http://www.centralbank.go.ke/downloads/bsd/annualreports/bsd2009.pdf>

CBK (2010b), *Annual Report 2010* for Period ending 30th June 2010 from <http://www.centralbank.go.ke/downloads/publications/annualreports>.

Goodman, S.E. and Lin H.S. (eds), (2007), *Towards a Safer More Secure Cyberspace*.

Committee on Improving Cyber Security Research in the US. From www.nap.edu/catalog/11925.html.

Pati, P. (2008), *Cyber Crime*. From internet.

APPENDIX I
INTRODUCTION LETTER

University of Nairobi

Date.....

Faculty of Arts

Department of Sociology

To the Respondent,

Dear Sir/ Madam,

My name is Okwara I. N. and I am an M.A. (Sociology) student at the University of Nairobi. I am interested in learning about how the Cyber Crime Prevention Unit at the CID Headquarters can be developed to meet the needs of prevention of Cyber Crime in Kenya. This is a partial of the requirements for the award of Master of Arts Degree in Criminology and Social Order.

I wish to assure you that any information you give will remain confidential and will only be used for academic purposes. I would also like to inform you that you have the right to refuse to take part in the study or to answer any of these questions. I further wish to thank you for your voluntary and informed participation in this study.

Signed.....

Date.....

APPENDIX II

RESEARCH QUESTIONNAIRE FOR DETECTIVES AT CID CCU.

PART A - BACKGROUND INFORMATION /PERSONAL DATA

1. Respondent's Sex 1. Male 2. Female

2. Respondents Age

(a) 25 -31		1
(b) 32- 38		2
(c) 39 - 45		3
(d) 45+		4

3. What is your Designation?

- (a) Constable 1
- (b) NCO 2
- (c) Inspectorate 3
- (d) Gazetted Officer 4

4. How long have you served in the Police Force?

- (a) 1- 3 years 1
- (b) 4 - 6 years 2
- (c) 7 - 9 years 3
- (d) 10 - 12years 4
- (e) 13+ years 5

5. How long have you served in CID CCU?

- (a) 0- 1 year 1
- (b) 2 - 3 years 2
- (c) 4+ years 3

6. What is your highest educational attainment?

- (a) Masters Degree 1
- (b) Bachelors Degree 2
- (c) College Diploma/Certificate 3
- (d) Secondary Education 4

7. Describe to me how you were recruited and posted to this unit.
8. What training did you receive prior to your posting?
9. What training have you received after posting?
10. What responsibilities are you assigned in your present post?
11. What resources do you require to function effectively in your position?
12. Which of these resources are adequately supplied?
13. Which of these resources are not adequately supplied?
14. What causes this deficiency?
15. What role do you have in ensuring that you are adequately prepared and equipped for function?
16. What incidents/cases of financial crimes have you had to investigate since being posted to your position?
17. How many of these cases have occurred in the last:
 - (a) 1Year.....
 - (b) 6 Months.....
 - (c) 3 Months.....

18. What incidents or cases were you able to resolve?
19. What incidents or cases were you not able to resolve? Why?
20. What liaisons has your Unit established to support your work?
21. What liaisons have your Unit not established but are important for your operations?
22. In what ways do the deployment practices in your Unit support your work?
23. In what ways don't these deployment practices in your Unit support your work?
24. In what ways can the limitations in your operations/functions be addressed?

Thank you for your cooperation.

APPENDIX III

Key Informant Interview Guide for Officials from CCK, Computer Society of Kenya, the Judiciary and a Bank.

General information

Male or female

Organization, Designation, Length of service and Functions.

1. What incidents of financial crimes do you encounter in your position?
2. What is the frequency of occurrence?
3. Are there any liaisons between your organization and others in Cyber Crime prevention?
4. What are the mechanisms available for cyber crime policing and prevention in financial institutions in Kenya?
5. From your assessment, in what ways have these Structures/Mechanisms led to meeting the objective of prevention of financial based Cyber Crime?
6. What needs to be done to achieve success in eradication of financial based Cyber Crime?
7. What measures are relatively effective in preventing financial based Cyber Crime?