DEPARTMENT OF INFORMATION STUDIES

UNIVERSITY OF GHANA, LEGON

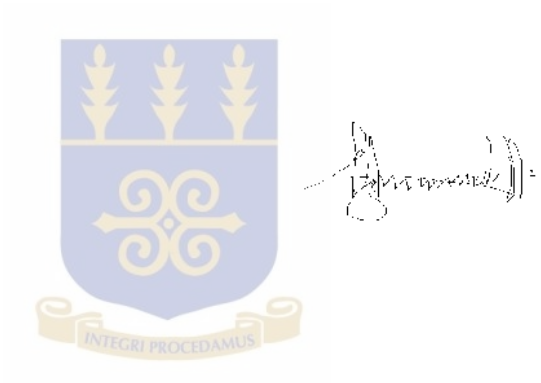
THE USE OF INFORMATION COMMUNICATION TECHNOLOGY (ICT) TO COMBAT FINANCIAL CRIME IN GHANA: A CASE STUDY OF THE GHANA POLICE SERVICE COMMERCIAL CRIME UNIT

BY

DAVID JOACHIM QUANSON

A DISSERTATION SUBMITTED TO THE DEPARTMENT OF INFORMATION STUDIES, UNIVERSITY OF GHANA, LEGON IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF ARTS IN INFORMATION STUDIES

DECEMBER, 2013



DEDICATION

I dedicate this work first to the Glory of God for the life and strength he gave me during this research. Secondly, to my supervisor Mr. M. D. Dzandu, my wife Gifty Quanson, the head of department, lecturers and the entire staff of the Department of Information Studies fortheir care, support and understanding.

ACKNOWLEDGEMENT

This dissertation would not have been successful without the support of certain personalities whose efforts have made the preparation of this work possible.

First and foremost, my thanks go to the Almighty God for giving me the breath and strength to come out with this study. I also want to render my profound gratitude to Mr. Michael Dzigbordi Dzandu, Department of Information Studies, University of Ghana Legon, who supervised this work and for his understanding when I encountered some personal problems whilst undertaking this work. His tolerance and accommodating nature must be mentioned. This work was made possible by Mrs. Gifty Quanson (my wife), and my children Litela, Nhyira, Linudja and Atiordi for their encouragement and support.

Not forgetting my humble lecturers Prof. E.E. Badu, Prof. A.A. Alemna, Prof. H. Akussah, Dr. Musah Adams, Dr. P. Akotia, Dr. Mrs. P. Dadzie and Mr. Edwin Ayenor for their encouragement and support.

The encouragements of the following co-workers of the Service: ACP Mr. G. A. Mensah, ACP Mr. A. Amponsah-Asiamah, Superintendent F.K. Mawuasi (head of Commercial Crime Unit), and Chief Inspector C.N. Nsiah (for holding the fort for me) May God richly bless them. Not forgetting my other colleagues whose immense encouragement and support saw me through this work.

I am also most grateful to Mr. Sampson Mark Amegayie of the University of Ghana, Department of Information Studies Library whose tireless efforts made this work possible. Finally, my warmest appreciation goes to my course mates Prince Owusu, Alex Asirifie, Eric Akuetteh Okleh, Mustapha Abdulllai and Godwin Ayekple among others for their tremendous support.

TABLE OF CONTENTS

LIST TABLES

LIST OF FIGURES

ABSTRACT

The rapid evolution of information technology, the proliferation of computer and media devices and the rapid growth in the use of ICT and the Internet for organisational management has brought new forms of crimes and made financial crime to be easier to commit. This study focused on the use of information communication technology (ICT) to combat financial crime in Ghana. It is a case study of the Ghana Police Service Commercial Crime Unit. The study used the Adaptive Information Security Systems model to serve as the basis for the literature review. To achieve the aim of the study, the survey methodology was used to survey thirty eight (38) respondents from the Ghana Police Service Commercial Crime Unit.

The study revealed that the use of ICT among the personnel was very low. The study also found out that the Service does not have the necessary ICT facilities to combat financial crime. Besides, the knowledge of the personnel of the unit in the use of ICT is inadequate. Therefore, the high hopes of ICT utilization and its resultant outcome is not realised.

Based on the findings, the study recommend that the Ghana Police Service in general and the Commercial Crime Unit in particular need to be resourced with modern ICT facilities and training of the personnel to be able to fight ICT-based financial crime.

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND OF THE STUDY

Information technology (IT) is playing a crucial role in contemporary society. It has transformed the whole world into a global village and changed global economy. Globalisation of world economies has greatly enhanced the values of information to business organisations and has offered new business opportunities (Singh, 2008).

Today, IT provides the communication and analytical power that organisations need for conducting trade and managing business at global level with much ease. To coordinate their worldwide network of suppliers, distributors and consumers, organisations have developed global information systems that can track orders, deliveries, and payments round the clock. This has been possible because of the development of ICT in its present form (Singh, 2008). In the broadest sense, information communication technology refers to both the hardware and software that are used to store, retrieve, and manipulate information.

Turban et al. (2011) contended that financial institutions are fast developing and producing millions of transactions daily stored in complex information systems. They further explained that efficient analysis of such large volumes of data is crucial for quick and real time decision-making. Product management, loss prevention and detection and suppression of fraud are also of concern to such financial institutions. With the current global issues of financial crimes, business stakeholders, law enforcement agencies and the government have also become more concerned with the security of business transactions and the far reaching repercussion of financial crimes on the image of the country in attracting foreign investment.

Financial crime is causing economies to lose huge amounts of money; The United Nations Office on Drugs and Crime (2005) has stated that $1.6 trillion 'dirty' dollars are floating around the global economy; the latest annual statistics from the UK's National Fraud Authority show that more than £38 billion has been lost over the last 12 months due to fraud (Sourcingfocus.com, 2012). Consequently, these days, financial institutions tend to seek means for secured and efficient analysis of their data (Saunders and Cornett, 2008). Adopting Business Intelligence (BI) tools can provide technological and innovative support in such cases, especially in developing countries like Ghana (Petrini and Pozzebon, 2003).

Financial crimes in Ghana have dominated the list of challenges business are confronted with as a result of their increased use of Internet-based IT solutions and systems. Ghana Business News (2012) reports that the Financial Intelligence Centre of the (Central) Bank of Ghana received a total of 206 Suspicious Transaction Reports in 2012 alone which were forwarded to law enforcement agencies to investigate. Also, the Criminal Investigations Department of the Ghana Police Service has launched the E-Crime Project to build the capacity of detectives in cybercrime investigation and intelligence gathering (Ghana Business News, 2012). With these two preliminary instances, it is prudent to say that organizations and the relevant stakeholders in Ghana are taking steps to deal with financial crimes.

In today's fast paced world, it is imperative for security personnel and journalists to be armed with proper and efficient tools to respond to ever changing and unpredictable situations they encounter in performing their duties (Muhammed-Nasiru and Kasimu, 2012). Considering contemporary developments in the technological world, surveillance serves as a valuable and essential tool for information gathering in combating criminal activities and security management in a country.

As observed by McQuail (2005), police and intelligence services are paying more attention to the need for combating financial crime especially in respect of potential trans-border crime, money laundering, cyber crimes and many new kinds of ICT crime. Conventionally, within any society or country, information gathering and combating crime by police exist for the purpose of security of lives and property. Information and communication technologies (ICTs) have revolutionalized every aspect of human endeavours. Today, ICTs promise a whole new and interesting horizon characterized by boundless possibilities and opportunities in the face of the continuous emergence of sophisticated tools, systems and approaches being adopted by IT criminal.

Information and communication technologies are the nervous system of contemporary society, 'transmitting and distributing seasons and control information and interconnectivity, a myriad of independent units' (Negash, 2004). Operationally ICTs are used for transferring information. It includes low-cost means of communication, like radio, GSM/mobile phones, and digital television-not leaving out the Internet. The set of technology is technically electronic machines devices and their application that have both computing and communication capabilities. Institutions and government agencies such as the Ghana Police Service and many other private security companies involved in combating financial crime can exploit the computing and communications power of IT to curb if not deal effectively with the alarming rate of financial crime in Ghana.

1.2 Profile of Ghana Police Service

Policing in Ghana (then the Gold Coast) was originally organised by traditional authorities led by local kings or chiefs. This, they did by employing unpaid messengers to carry out executive and judicial functions in their communities. Professional policing was introduced

by the British Colonial Authorities to the Gold Coast now Ghana in 1821 (Pokoo-Aikins, 2002).

The Criminal Investigations Department (CID) was established in 1922. Following the riots of 1948 led by the Big Six, the Special Branch and the Police Reserves Unit was formed for riot control and to prevent destabilisation of the government. The Special Branch was to gather intelligence. The Wireless and Communications unit was opened in June 1950. A women's branch was established with officers in 1952. The Police College was opened in 1959. Prior to this, all officers were trained in the United Kingdom.

The first Ghanaian to head the Ghana Police was E.R.T. Madjitey, who was appointed on October 9, 1958 by President Nkrumah. The Ghana Police Service (GPS) is the main law enforcement agency in Ghana. The service was established to perform functions such as the detection of crime, the apprehension of offender, the maintenance of law and order and the maintenance of internal peace and security. In order to perform these functions, it is the stated that the mission of the police is to ensure operational readiness and make available trained police personnel for deployment at all times throughout the country (Pokoo-Aikins, 2002).

The Ghana Police Service (GPS) has a unitary command under the Inspector-General of Police (IGP). Although there are many regional and divisional commands, they all report to the national headquarters in Accra. The GPS is organised under the IGP who has two deputies, Deputy IGP's responsible for administration and operations respectively. Again the Service structure is organised at national level into ten schedules, each headed by a commissioner. The schedules include:-operations which comprises of Criminal Investigation Department (CID), Legal and Support Services, operations and recently introduced Police Intelligence and Professional Standards Bureau (PIPSB) and Administration on the other

hand has Human Resource Development, Welfare, Research, Planning and Information Communication and Technology, Strategic Direction and Monitoring and Finance.

There are a number of regions under the Service. Each of them is headed by a Regional Commander. These are the ten geographical regions: Ashanti, Brong Ahafo, Central, Eastern, Greater Accra, Northern, Upper East, Upper West, Volta and Western Regions. The last three regions are Tema, Railway and Ports, and finally National Headquarters. Apart from the preceding, as a result of the oil discovery, the Service has established the Marine Police in the Western region. With the exception of the National Headquarters the regions are divided into 51 divisions nationwide. These divisions are further subdivided into 179 Districts and 651 Stations across the country.

The Criminal Investigation Department (CID) has eleven (11) units engaged in the investigation of various crimes under it. The units are the Anti Armed Robbery Squad (AARS), Homicide Unit (HM), Anti Human Trafficking Unit (AHTU), Auto Theft Unit (ATU), Commercial Crime Unit (CCU), Criminal Data and Statistical Bureau (CDSB), Forensic Laboratory (Crime Lab), Document and Visa Fraud Section (DVS), Criminal Vetting and Profiling (VCA), Property Fraud Unit (PFU), Firearms, Sale and Licensing (FSL) and Court Unit.

The CCU which is the main focus of this study has evolved overtime with the following names. It was first called Flying Squad, then Fraud Squad. It changed from the latter to Economic Crime Bureau and currently it is called the Commercial Crime Unit (CCU) (Pokoo-Aikins, 2002).

This study attempts to evaluate the use of information communication technology (ICT) to combat financial crime in Ghana by using Ghana Police Service Commercial Crime Unit as the case study.

1.3 Organisational framework of the Commercial Crime Unit

The organisational framework of the Commercial Crime Unit (CCU) of Criminal Investigation Department (CID) Headquarters, Accra is a unit that investigate all crimes in Ghana. It is headed currently by a Superintendent of Police. The second and third in commands are a Superintendent and Assistant Superintendent respectively. The Unit has the following sections investigating special crimes such as:

i. Cyber Crime
ii. Document and Visa Fraud
iii. Property Fraud
iv. Auto Theft and
v. Intellectual Property Fraud.

All these sections have senior Police Officers as Heads. The Superintendent of CCU supervises the activities of the Unit. The unit receive cases referred by the Director-General of CID. Cases from all over the country and International Police Organisation in which people and organisations referred to the Unit for investigation.

The Unit reports directly to the Director-General/CID.

Policy

The policy of the Criminal CID is what prevails. The Commercial Crime Unit (CCU) has no unique policy apart from what the CID has in place. However, on the issues of criminal investigation, the approach to arraign all cases of fraud involving gold before court if there is evidence.

Standards

Commercial Crime Unit maintains professional standards in the Unit. New detectives posted to the Unit are mentored to maintain high professional standards. This is by encouraging personnel to do thorough and effective investigation, to handle clients in a polite manner at all times and to deal with colleagues with utmost respect.

Practices

The Commercial Crime Unit (CCU) engages in criminal investigation which relates to cyber crime. This involves evidence gathering mainly. And it requires a lot of resources in Information Communication Technology (ICT). However, the Unit regrettably lacks these resources. For instance, CCU does not have reliable Internet facilities. This retards investigation of Internet-based crimes.

1.4 Statement of the problem

The speed with which information communication technology (ICT) is developing and its impact on socio-economic activities cannot be overemphasized. It is imperative that Ghana is not excluded from the technological revolution. It is a stark fact that the use of ICT has been integrated into virtually every facet of commerce, education, governance and civic activity has become a critical factor in creating wealth worldwide. Unfortunately in Ghana, ICT has barely taken a foothold. Computer illiteracy and lack of access to ICT are widely recognised as an increasingly powerful obstacle to the economic, civic and political development of Ghana. This is where Ghana as a country finds itself.

Recently, Ghana signed an agreement with Microsoft Corporation under which the largest and richest ICT Company in the world would provide resources to improve ICT education in Ghana. To recap, it is important to note that Ghana in 1995 became the first country in the Sub-Saharan Africa to have full Internet connectivity.

Though Ghana is not yet there as far as ICT infrastructure is concerned, it has been able to chalk some successes in attracting some foreign investors to the country. Some of them are Affiliated Computer Services (a Fortune 500 company and a global leader in IT and Business Process Outsourcing), Data Management International Inc., Rising Data Solutions, Global Response, Busyinternet, AQ Solutions and Supra Telecom. Most of these companies operating in the country have recorded an average of 50% in revenue and profits. Other U.S companies like Cincom System Inc. a call centre and Convergys Corporation are expected to open offices in Ghana.

However, despite these massive investments in ICT infrastructure and ICT capacity building, Ghana is to a large extent digitally isolated from the Global Village because it lacks the critical drive and strategies to harness the full potential of ICT for the socio-economic development of the country. These have been some of the challenges facing the full ICT deployment in the country. Ghana Telecom, the national carrier that is supposed to be at the forefront of ICT development to assist the Commercial Crime Unit of Ghana Police Service is struggling and has failed to keep up with the times. For the past years, the carrier has faced a number of challenges. These range from Voice-over IP and international traffic termination issues.

The Commercial Crime Unit of Ghana Police Service in recent time has been receiving numerous reports on financial crimes committed either against individuals, private businesses or financial institutions through the use of ICT-based systems. Dealing with these complaints poses a challenge to the Commercial Crime Unit of Ghana Police Service as most of the ICT facilities present are in the deplorable state and lack ICT skilled personnel to handle the issues.

Coupled with the above problems is that the Commercial Crime Unit of the Ghana Police Service does not have modern ICT facilities not to talk of Internet connectivity which is only now underway, creates a huge problem for the unit to deal efficiently with problems of ICT-based financial crime.

1.5 Purpose of the study

The purpose of this study is to examine the use of information communication technology (ICT) to combat financial crime in Ghana and to identify possible problems and to make recommendations.

1.6 Objectives of the study

The research thus seeks to:

i. examine the regulatory framework-ICT Policies, standards and the ICT facilities currently in use for combating financial crime in Ghana by GPS.

ii. determine the type and level of financial crime activities in Ghana.

iii. determine the adequacy of the available ICT's for combating financial crime

iv. assess the level of use of these ICT facilities to combat financial crime?

v. ascertain the competency level of the GPS in using ICT for combating financial crime in Ghana.

1.7 Research Questions

The following are the research questions emanating from the research objectives.

i. Is there a strong and effective regulatory framework?

ii. What types of financial crimes are being committed?

iii. Does the Police administration have enough ICT facilities to combat financial crime in Ghana?

iv. Are these ICT facilities being used or under used to combat financial crime?

v. Are the personnel competent to use the ICT facilities to combat financial crime?

1.8 Scope of the Study

The study focused on Commercial Crime Unit of the police administration, looking mainly into ICT facilities usage for combating financial crime. The Commercial Crime Unit of the police administration was selected because the researcher believes that this unit deals with ICT utilization and commercial crime activities in the country and it has a sizeable number of personnel that would give a clear picture of the adoption of ICT and some of the difficulties encountered when using the facilities in combating financial crime and for that matter the findings of the study could be generalised. Ideally, the study should have covered the entire

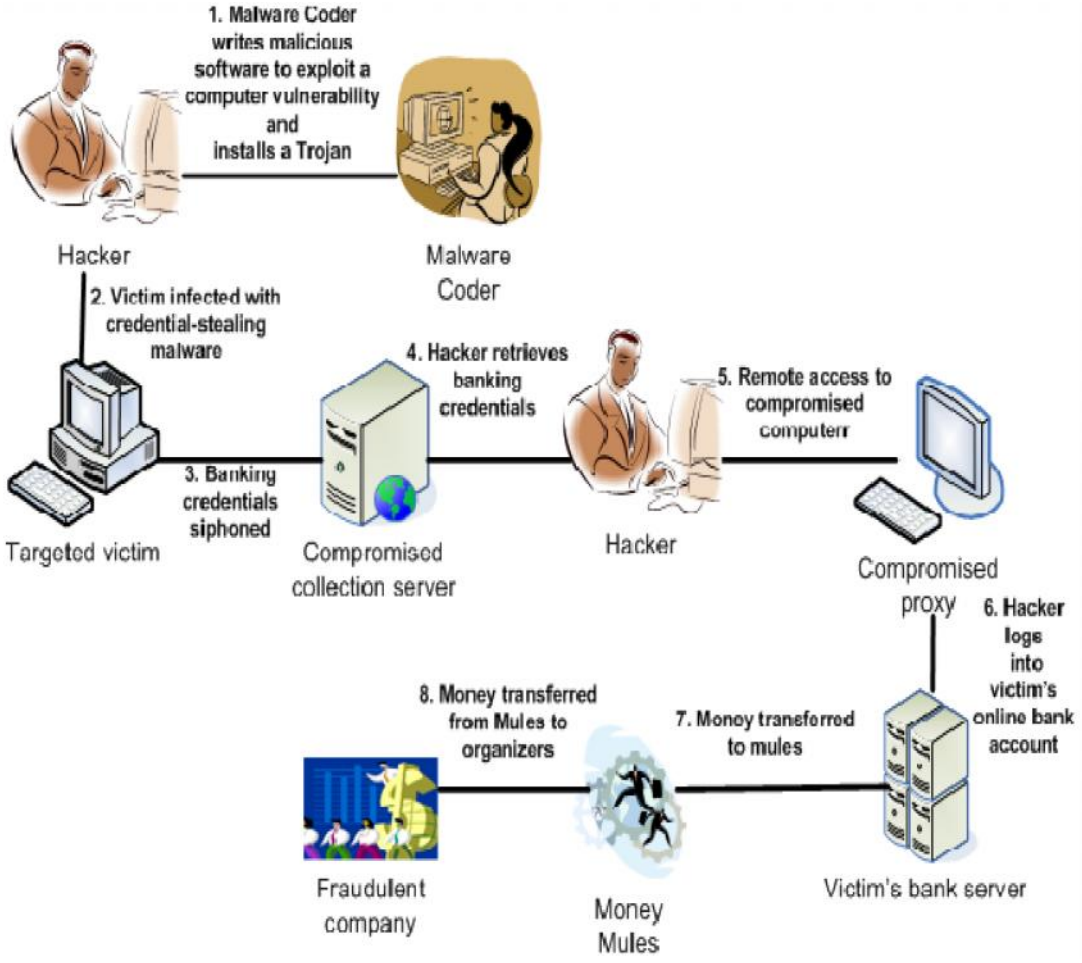
country, however, this would have been extremely difficult considering the time and other resources involved.

1.9 Theoretical framework

Several theories have been propounded with regard to the use of information systems and these include Theory of Reasoned Action (TRA), Diffusion of Innovation (DOI), Theory of Planned Behaviour (TPB), User Acceptance Theory (UAT) and Technology Acceptance Model (TAM). For the purpose of this study, the adaptive information security systems model was adopted for the study because it provides stages on how ICT is being used to commit financial crime.

This conceptual framework seeks to buttress the issues raised in the adoption of best practices of Ghana Police Service with respect to the use of ICT in combating financial crime. Mwakalinga and Kowalski (2011) claimed that there is much to be learned from the activities of other security institutions that have been, or are, engaged in similar efforts at fighting financial crime process. Even though this contribution is valid there could be certain problems associated with it and these are an organization could blindly follow the practice of the other agencies or institution in sense that they may not be aware of the process these used. Also the fact that a strategy worked in one agency or institution does not mean that it would work for institution. One needs to identify the problem within the institution such as how fraud works. This framework will enable the Police institution to trace the root cause of the use of ICT in financial crime and find a solution to it.

Unlike other theories, the adaptive information system model will provide efficient ways to address the problem and provide the desired outcome for the Commercial Crime Unit of the Ghana Police Service.



In Figure 1, the first step criminals take to commit financial crime is to introduce a malicious coder that created a Trojan horse called Zeus (Mwakalinga and Kowalski, 2011). Study conducted by FBI in 2010 revealed that hackers do inters banking software by writing official looking letters and sent them to small and medium sized companies and if the letter is open then the Trojan captured the banking credentials and within a short time transferred can be done electronically to the bank accounts.

In step 2, the hackers installed the Zeus Trojan in victims' computers via e-mail attachments. When this is Trojan is install then it acted as social engineering by convincing the victim that the email and the attachment was an official letter from a fellow employee. At this stage, the adaptive model would have prevented the Trojan to run because no program without a special identity, authorization, and registration in the program database would be allowed to run in the computer. There are software agents in the adaptive model that monitor and check the authentication and authorization of every programme, which tries to run.

In step 3, the Trojan horse captured bank accounts, passwords, and other credentials for login into financial accounts and stored them in a compromised collection server. The method used here is monitoring and recording the banking credentials. The adaptive model has agents for monitoring the actions of the programmes running on a computer. The adaptive model could have detected the actions of the Trojans. The victim's computer and the collection server lacked deterrence, prevention, detection and response measures both social and technical measures.

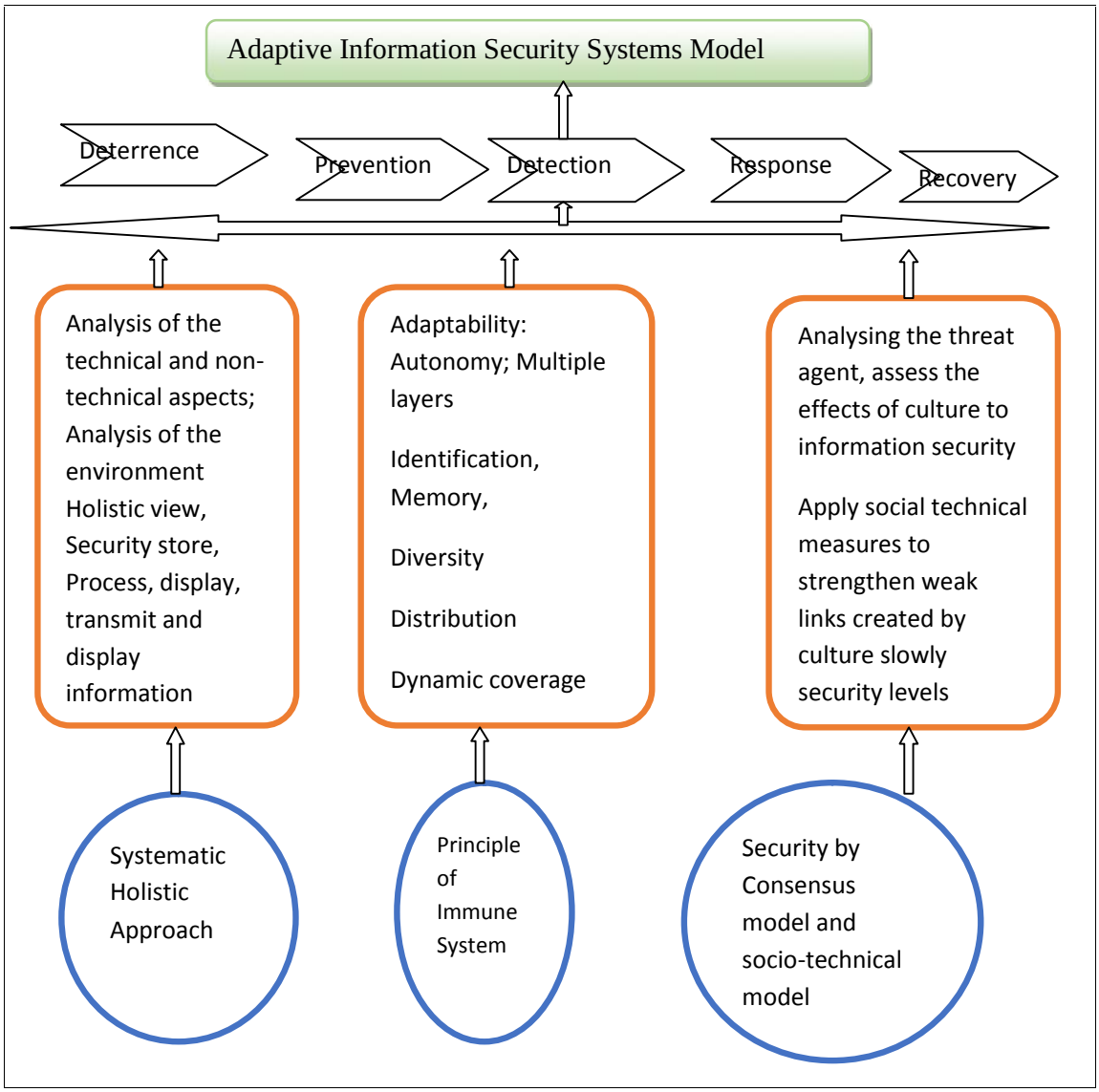
In step 4, the criminals retrieved banking credentials. In this step, the adaptive model has agents that detect the information that is sent out; the ports used, and check the programs that are sending the information. Here there was no program to detect what was sent out.

In step 5, the criminals remotely accessed the compromised proxy. The compromised proxy lacked deterrence, prevention, and detection, and response measures. The identification, authentication, authorization, confidentiality security services are not working properly in the compromised proxy. Therefore, the hackers can be able to compromise and access it, and then used it as a proxy to log to the victim's bank.

In step 6, the criminals log into victim's online bank account and transfers money without authorization. The method used is impersonation using the banking credentials that were captured by the Trojan. When the bank system lacks strong deterrence, prevention, and detection measures to scare away criminals, or prevent and detect their activities then the security services authentication, and authorization are not strong to detect the criminals.

In step 7, money then been transferred to money mules. The mules create bank accounts using fake documents and phony names. The mules may have been registered fake company an address of an unmarked, building so it cannot be detected immediately. In this case when the identification, authentication, authorization, non-repudiation, detection, prevention, and response measures are weak, the systems may not detect the fake documents and phony names when accounts are been created accounts, the system supposed to respond immediately. In addition, when the amounts that were supposed to be withdrawn using ATM cards were raised the banking detection systems must detect, react, and inform the bank. Figure 2 next page show the Adaptive Information Security Systems Model.

Figure 2: The Adaptive Information Security Systems Model



Source: Mwakalinga and Kowalski (2011)

The model consists five critical systems the deterrence, prevention, detection, response, and recovery. According to Mwakalinga and Kowalski (2011), every business institution must have a model that can act as a security manager of the company or to be able to prevent financial crimes there is the need for financial institutions to have adaptive information security systems model in their computer systems for identifying potential victims. To Mwakalinga and Kowalski (2011) the adaptive information security systems model consists of critical sub systems to protect every transaction that must take place in the system.

1.10 Significance of the Study

It is believed that the study will be beneficial to the following stakeholders in Ghana. Financial Institutions: these will be given more insight into financial crimes and on Business Intelligence as an effective tool for data analysis and decision-making. Business Users (analysts, information managers, consultants): These will be updated on current information management practices that will help them improve the business processes of their organizations.

The study will also contribute to already existing knowledge in the area of the study, useful to researchers and scholars, as it would add to the scholarly research and literature in the field. The study therefore, will help identify how ICT resources could be adopted by the Ghana Police Service in combating financial crime in a more efficient way without regard to distance. The study is intended to find out how ICT could help the police service especially commercial crime unit to enhance and improve their service delivery.

In general, the study will help establish the need for the integration of ICT fully into the processes of police administration in Ghana. Thus, police personnel, researchers, ICT professionals, and financial institutions stand to benefit from this study. The study will provides insight of ICT utilization in the police service.

Finally, the results of the study provides policy and decision makers with a considerable knowledge on contemporary issues of adopting ICT resources, it will provide the Ghana Police Administration with the benefits of adopting ICT as appropriate measures for combating crime in general in Ghana.

1.11 Organisation of the Study

The study is organised into five chapters:

Chapter One covers the introduction giving a background to the study. It includes the research setting which is the overview of Ghana Police Service, statement of the problem, purpose statement, objectives of the study, research questions, scope and limitation, theoretical framework, significance of the study and the organisation of the study.

Chapter Two covers the literature review of relevant literature on the topic.

Chapter Three deals with the methodology adopted for the study, which covers the research design, population, sample technique, instrumentation, mode of data collection and mode of data analysis.

Chapter Four covers the data analysis, result presentation and discussion of the findings.

Chapter Five, the final chapter, provides the summary of findings, conclusions, recommendations.

REFERENCES

Abor, J. (2004). *Technological Innovations and Banking in Ghana: An Evaluation of Customers' Perceptions. American Academy of Financial Management*. Retrieved from: www.financialanalyst.org, (Accessed on: January 28, 2013).

Akussah, H. (1994). *An Automated National Records Centre Management System for Ghana: A Feasibility Study*. An unpublished Msc Dissertation Submitted to the School of Library, Archives and Information Studies, University College London.

Negash, S. (2004). Business intelligence. *Commun. Association Inform. Syst*., 13: 177-195.

Ghana Business News (2012). *Ghana Police Launches E-Crime Project*. Retrieved from: http://www.ghanabusinessnews.com/ghana-police-launches-e-crime-project, (Accessed on: January 30, 2013).

Ibezimako, M. (2006). Information and Communication Technologist (ICTs) in Modern Public Relations Practice: Uses, Impact: in Mass Media Review. *An International Journal of Mass Communication*, p.84.

Leman-Langlois, S. (2008). *Technology, Crime and Social Control*. Manitoba: Willan Publishing.

McQuail, D. (2005). *Communication Theory* 5th Ed., London: Sage Publication.

Moin, I.K. and Ahmed, B.Q. (2012). Use of data mining in banking. *Int. J. Eng. Res*. Appl., vol. 2, No.2, pp. 738-742.

Muhammed–Nasiru, I. and Kasimu, S. (2012). *Surveillance, Information and Communication Technologies (ICTs) as Tools for Information gathering and Security Management*.

M.A dissertation, Department of Mass Communication, School of Information and Communication Technology (ICT), Auchi Polytechnic, Auchi.

Mwakalinga, J. and Kowalski, S. (2011). ICT Crime Cases Autopsy: Using the Adaptive Information Security Systems Model to Improve ICT Security. *International Journal of Computer Science and Network Security*, 11(3): 1-10.

Myjoyonline.com (2012). *Police turns to ICT to fight crime. General News of Saturday, 18 February*. Retrieved on 03/12/2013 from http://www.ghanaweb.com/GhanaHomePage/NewsArchive/artikel.php?ID=230212

Paulsen, D.J. (2009). *A Discussion of Technology and those who use it for criminal gain*. Retrieved on 28/11/2013 from http://www.criminalbehavior.com/Spring2009/Section%201%20Hackers.pdf

Petrini, M. and Pozzebon, M. (2003). *The value of "business intelligence" in the context of developing countries. Proceedings of 11th European Conference on Information Systems*, Napoli, Italy.

Rogers, M. (2001). *A new hacker Taxonomy*, *Department of Psychology University of Manitoba*, Winnipeg RSA Security Conference.

Saunders, A. and Cornett, M. (2008). *Financial Institutions Management: A Risk Management Approach* 6th ed. New York: McGraw-Hill, p.2.

Singh, R.S. (2008). *Encyclopaedia of Library Science Today*. New Delhi: ANMOL Publications PVT. Ltd.

Sourcingfocus.com, (2012). *UNISYS: Using Big Data Analytics to Fight Financial Crime*. Retrieved from:

http://www.sourcingfocus.com/uploaded/documents/Unisys_Using_big_data_analytics_to_fight_financial_crime.pdf (Accessed on: November 30, 2013).

Pokoo-Aikins, J.B. (2002). *The Police in Ghana 1939-1999*. Accra: Rescue Printing Press.

United Nations Office on Drugs and Crime (2005). *Bi-Annual Seizure Report 2004/2'*. UNODC, April 2005. Retrieved on 07/12/2013 from http://www.unodc.org/pdf/WDR_2005/volume_1_web.pdf

Turban, E., Sharda R., and Delen, D. (2011). *Decision Support Systems and Intelligent Systems* 9th ed. New York: Prentice Hall International.

van Soomeren, P. (2000). *Crime prevention solutions for Europe: Designing Out Crime, Conference on the relationship between the physical environment and crime reduction and prevention*, Szczecin – Poland.

Victorian Auditor-General's Report (2012). *Obsolescence of Frontline ICT: Police and Schools*. Retrieved on 03/12/2013 from http://www.audit.vic.gov.au/publications/20120620-ICT-Obsolescence/20120620-ICT-

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter reviews literature from various sources including textbooks, the internet, magazines and other sources. According to Taylor (2012), literature review is a description of literature relevant to a particular field or topic. It gives an overview of what has been said, who the key writers are, what are the prevailing themes and hypothesis, what questions are being asked and what methods and methodologies are appropriate and useful.

Literature review is important because it reports on other findings, seek to describe, summarise, evaluate, clarify and or integrate the content of primary reports. It may be purely descriptive, as in an annotated bibliography or it may provide a critical assessment of the literature in a particular field, stating where the weakness and gaps are, contrasting the views of particular authors or raising questions, summary that evaluate and show relationship between different materials.

In reviewing literature, the researcher draws attention to the following subheadings: the role of ICTs in fraud, financial crime situation in Ghana, computer crimes in Ghana, implications of computer crimes for organisational management, the Impact of ICTs on information gathering and security management, ICT surveillance and the law of invasion of privacy, the Significance of ICTs on information gathering and security management and summary.

2.2 The role of ICTs in fraud

It is not a paradox but common sense, that the same technology which allows parallel opaque financial systems to exist may be the key to change this state of affairs. This is the main lesson to extract from an important investigation embodied in two books that have had hardly any impact on the public opinion: Rao and Dey (2012) and Salwan (2008). Both books are written by French researcher and journalist Denis Robert, who describes a long and dense investigation proving, amongst other things that the weakness of the criminal financial system stems from the very strength of the system --- that is, from ICTs use. To understand this we must first talk about contemporary history of the financial systems and the meaning of clearing.

According to Dugo (2008), during the early 1970's, several banks established around the world decided to associate and set up an inter banking cooperative. At that time they were only a hundred (today they add up to more than two thousand) and their objective was to create a system to facilitate international banking exchanges, which would be called clearing. Rao and Dey (2012) explains it in this way: Let’s go back some decades. When an insurance agent from Chicago wanted to sell part of his company's capital to a Greek ship-owner, how did he do it? He went to see his banker, let's say the Bank of New York, and confided to him the task of selling the bonds. The banker took a plane to Athens, where he was going to meet with the shipowner’s banker, for instance the Greek subsidiary of the ABN AMRO Bank. Clearing allows, on one hand, to save time, and therefore, money. It is not necessary to travel. From then on, a central organization has guaranteed the happening of the exchange. The basic principle is trivial: bankers from different countries should join to create a confidence area where the banking exchange will be registered and guaranteed. Unlike the stock exchange market, which brings together the different elements of a transaction, a clearing company is

an infrastructure apparently passive. It takes care of registering and guaranteeing the modification.

The bonds do not move, only the name of the owner is changed (Rao and Dey, 2012). The clearing system, also known as 'compensation systems', pretended to bypass the minimum two weeks which the foreign buyer had to wait before the bonds arrived (for instance, a Rome bank buying IBM shares from a bank in New York, as requested by a client). It was aimed at avoiding time and money costs (the shipment had to be insured, and precious time was wasted while the bonds were physically travelling).

According to Rao and Dey (2012), the first clearing society, Euroclear, was created in 1968 in Brussels and was founded by an American bank, Morgan Guaranty Trust Company of New York, which at the time was the biggest private bank in the world. The second clearing society appeared in 1970, called Cedel (now Clearstream), as a reaction from the European or American banks who had not participated in the creation of the first clearing society. These are, until now, the two only current transnational clearing societies. Euroclear and Clearstream allowed their member institutions to exchange titles (shares, securities, and the like) to balance their accounts after performing operations at their own risk or on behalf of their clients. Their success was such that all current important international transactions are now dealt through one of these two societies exclusively. A compulsory step that involves the almost real time recording and storing of a footprint of a transaction in codified documents were born (Rao and Dey, 2012).

Although these are the only two clearing systems at a cross-border level in the world, clearing systems exist at the national level almost in any country. Their tasks are limited to domestic compensatory operations of capital exchange, and the amounts of money shifted around by the national societies cannot be compared at all to those of the international societies. In

December 2004, Clearstrem alone claimed to be performing 250,000 transactions daily (the total number of international transactions processed by Clearstream rose to 17.2 million throughout 2004), while the value of assets held in custody on behalf of customers rose to approximately EUR 7.6 trillion (Bureau of Justice Assistance, 2009).

In summary, since the 1970s, clearing 'has learned to make itself discretely essential' (Rao and Dey, 2012), and has been progressing in close association with economic liberalization. 'Clearing has contributed to the foundation of what economy and financial journalists have christened as the Global Village (much later after bankers and clearing users adopted Marshall McLuhan's term a village where power and information centres are interconnected' (Rao and Dey, 2012). Currently, there is no important international transaction that is not channelled through one of these two big companies, Euroclear and Clearstream. The clearing system has become, by mouth of an ex-official of Clearstream, 'the world's notary' (Rao and Dey, 2012).

Sure enough, the rulers of the clearing societies are the new world's digital notaries. Every single international or national financial transaction is registered there, and anyone trying to avoid the clearing societies risks ending up outside the world's banking system. That is, international clearing systems are the mechanisms of mutual confidence created by banks so they have a chance to play on the world's financial field. It is an organized system that has accompanied the explosion of financial markets, and here you have the big discovery by Denis Robert: clearing has superbly adjusted to the interest of some key groups. Robert, with the help of an insider from one of the two big cross-border clearing societies, Ernest Backes, co-author of one of his books, concludes that these systems are an ideal method for money hiding and laundering, and that it is in this way how they are being used. Thanks to a

perversion of the clearing systems --- states Robert --- fraud opportunities at the international level are made much easier, making them practically undetectable. But, even if undetectable and invisible for public control, they still exist and can be prosecuted.

Robert and Backes describe details for this with a wealth of evidence. They reveal how both clearing societies use the undisclosed accounts system (created for a particular legitimate use) to hide certain transactions. Transactions carried out in these undisclosed accounts represent, according to Robert and Backes, a tremendous opportunity for those seeking 'maximal discretion in the global village' and succulent profits for the clearing society. Further, they state: We have been able to establish that most of the accounts managed from tax havens, especially those from large European and American banks, are undisclosed accounts. We can interpret this as the search for maximum discretion, in this way, a double security lock. Not only do they create a subsidiary in a tax haven, but they also provide it with undisclosed accounts (Rao and Dey, 2012).

Greer (2010) contended that although Clearstream and Euroclear were created to speed up the exchange of equities and to avoid the physical transfer of titles and money, this would have not been possible without the fundamental role of ICTs. Essentially, computing and telecommunications enabled the creation of clearing societies, which in turn guarantee their management. All clearing societies keep records of every single transaction performed. Even if pretending not doing so, it would be absurd, as this is their safety guarantee against their most influential clients. It is the use of this sophisticated technology that makes these societies trustworthy; it is precisely their technology that allows managing the complexity of the system and keeping it under control. Any judicial or criminal inquiry about international crime would be able to progress drastically if it would have open access to the registries of these two big societies.

According to Rao and Dey (2012), ICTs are related to such a degree to the creation and maintenance of the financial world core that the main instrument of these clearing societies is itself a technology company: The Society for Worldwide Interbank Financial Telecommunication (SWIFT). SWIFT was created by the main shareholders of the two international clearing systems (a group of 239 European and North-American banks) in Belgium in 1973.

Rao and Dey (2012) posits that SWIFT belongs to more than 3,000 banks and connects more than 7,600 financial institutions. The aim of creating SWIFT was to provide clearing societies with an instrument for extra fast transmission of cash in every currency. Nowadays, nearly all the banks in the world are connected by means of this system. SWIFT is the technology platform that links all the world's financial institutions and that is used by the two big clearing societies. According to data from the company itself (11), in 2004 the SWIFT world network transferred several billion dollars a day for the 3.5 million messages negotiated daily (which meant more than 2,000 million messages negotiated that year). And, anything can be found in the SWIFT channels, 'from a Serbian dictator's bank to that of an Iraqi chemical weapons dealer, including the investment society of a Colombian dealer or the broker company from a Panamian shipowner' (Rao and Dey, 2012).

However, the clearing societies and SWIFT are not the only link in the chain for those wanting to launder money. An accomplice entry bank that is ready to risk accepting doubtful funds must be involved. But this is not a problem thanks to tax havens. (Rao and Dey, 2012) goes further in stating that 'tax havens would not exist without large trading banks and without the international clearing societies belonging to these large trading banks' (Rao and Dey, 2012). He adds to this that the growth of offshore systems is nearly paralleled by the growth of the clearing system:

Nowadays, most of the literature in this subject report up to at least fifty per cent of the world financial movements as circulating through tax havens. The comparison with the increase in power of the international clearing is surprising (Rao and Dey, 2012).

According to this investigator: The dreadful couple international clearing-banking haven offers extra protected opacity pockets only accessible to the initiated: secret services or ministries, but mostly, banks, multinational companies, turbid companies (Rao and Dey, 2012). In short, ICTs enable reliable and safe interconnection of finances around the world. But this interconnection belongs to the private hands of the interconnected agents themselves, which has led to 'unsustainable diversions to the detriment of transparency in the markets' (Rao and Dey, 2012). The pretended self-regulation of the financial markets and the agreements amongst some large banks and multinational companies, trying to hide their benefits, has added to the substantial profits arising from managing gains related to terrorism and drug dealing. This has led to the perversion of the system which, still working for its legitimate original purpose, has suffered an illicit broadening of its uses. But, at the same time, clearing societies offer an ideal point of view: they are the perfect vantage point over the financial markets.

Schneider and Enste (2000) said, a popular argument amongst politicians and economists regarding organized crime, and more specifically, financial crime, is the impossibility to control world transactions. This is the main reason why, for instance, critics of the Tobin Tax (13) consider it impossible to apply. However, the ad fundum knowledge of the real function of financial markets leads to quite different conclusions: it is perfectly possible (and relatively easy) to accurately quantify the daily value of international financial transactions.

The most important financial transactions are cleared and recorded electronically by only two international clearing societies (the national transactions are in the corresponding national

clearing societies). The reliability and accuracy of such exchanges has to be guaranteed, otherwise the system would not be safe and reliable enough to be used by its own users and clients (Schneider and Enste, 2000).

Therefore, it should not be a problem to claim a tax for international transactions, to control the main financial movements in the world, or to ascertain the whereabouts of large sums of vanished money, as long as the international clearing system made its technological platform accessible to magistrates, the police, politicians and citizens. When a journalistic source speaks about an enormous volume of illegal or crime related money that is vanished and that evades justice, what this source should rather talk about is money 'protected within the opacity' in which clearing societies work. Money is not evaded, what has been evaded are legal responsibilities. The reason is simple: clearing - the real functioning of the markets, the technological foundation for world finances… is an absolute unknown.

2.3 Financial crime situation in Ghana

According to the Daily Guide (2013), financial crime situation in Ghana is in the form of fraud and money laundering. As reported in Daily Guide (2013) Richard Kumadoe who is the Executive Director of Quest Services Ltd has urged banks and other financial institutions to efficiently prevent criminals from using their facilities to perpetrate fraud. "Combating these financial crimes and fraud is a perpetual battle with criminals leveraging the latest technology and strategies to circumvent the defences of financial institutions and the state. The Executive Director of Quest Services Ltd, a due diligence and risk management centre, told CITY & BUSINESS GUIDE last week after an anti-fraud workshop for bankers that the ongoing coverage of financial crime in Ghana indicates that the fraud landscape continues to evolve. Those tasked with fraud detection and prevention must keep pace with the modern trends, yet

many of our institutions and investigators rely on legacy platforms that cannot handle today's volume and complexity of fraudulent activity and as a result, fraud is everywhere and virtually every entity suffers from it resulting in the state and its allied institutions losing millions yearly," he said. He pointed out that "anti-fraud teams need the capability to connect the vast quantities of available structured and unstructured data in a way that allows them to rapidly identify and prioritize fraudulent activity for investigation as prevention and detection is much more effective and valuable than trying to recover losses after the act (Daily Guide, 2013).

The Executive Director said "the state and institutions must take immediate plans and implement proactive strategies in finding new ways to fight the fraud menace," Which he termed "Real-Time Fraud Detection Techniques. Our country and institutions have been engulfed with financial crime and fraud to the dismay of many. Recent trends have shown how the state has lost millions of the taxpayers' money in corrupt practices in GYEEDA at the time when the state needs so much money to fix the economy (Daily Guide, 2013).

Not only that but also financial institutions cannot be spared either, fraud everywhere, mostly covered and concealed from the general public's eyes for fear of losing their reputation and customers dissatisfaction of how much of their hard earned savings have been lost through fraudulent activities as a result of negligent practices by those who are supposed to know better (Daily Guide, 2013).

Sharing information and assisting law enforcement in investigations are some of the ways to detect, identify, prevent and analyse the impact of myriad fraud schemes. "We must all accept our distinct roles and responsibilities when it comes to fraud prevention in order to save our beloved country and combat financial crime from Corporate Ghana (Daily Guide, 2013).

To Aidoo, Akotoye and Ayebi-Arthur (2012) globally, cases of computer crimes date back to the early 1960s when the first case of computer crime was reported. Since then, there have been countless reports of computer crimes being made on a daily basis (Kabay, 2008). These early attacks often used unauthorised access to telecommunications systems to subvert long-distance phone systems which modified or destroyed data for financial gain, revenge, amusement and theft of services. Additionally, programmers in the 1980s began writing malicious software, including self-replicating programs, to interfere with personal computers.

With increased Internet access to increasing numbers of systems worldwide, criminals used unauthorized access to poorly protected systems for vandalism, political action and financial gain (Kabay, 2008). As the 1990s progressed, financial crime using penetration and subversion of computer systems increased (Rollins & Wyler, 2010). The types of malware shifted during the 1990s, taking advantage of new vulnerabilities. Illegitimate applications of e-mail grew rapidly from the mid-1990s onward, generating torrents of unsolicited commercial and fraudulent e-mail (Rollins & Wyler, 2010).

The President of the Accra Chapter of Information Systems Audit and Control Association (ISACA) commented at Information Systems Audit and Control Association (ISACA) IT Governance Summit 2011 in Accra that Ghana was failing woefully in its bid to regulate its Information Technology environment. He stated that: “even though the Data Protection Bill was recently read in Parliament, it is just one aspect of the bigger picture, since there’s no regulation or legislation that ensures the protection of government or listed company’s data” (BiztechAfrica, 2011). For example, absence of a cyber-law in Ghana is frustrating the efforts of the Vetting Crime Intelligence Analysis (VCIA) unit of the Ghana Police Service in fighting computer fraud and also to prosecute perpetrators of Internet fraud (Telecoms, Internet and Broadcast in Africa, 2007).

2.4 Computer Crimes in Ghana

According to Aidoo et al, (2012), ICT crime denotes the use of computers by individuals in one of three ways. Firstly, a computer may be the target of the offence. In these cases, the criminal's goal is to steal information from, or cause damage to, a computer. Secondly, the computer may be a tool of the offence. This occurs when an individual uses a computer to facilitate some traditional offence such as fraud or theft (for example, a bank employee may use a computer program to skim small amounts of money from a large number of bank accounts, thus generating a significant sum for personal use). Thirdly, computers are sometimes incidental to the offence, but significant to law enforcement because they contain evidence of a crime.

Aidoo et al, (2012) further contended that management of most organisations do not realize the value of prevention in the area of computer security, but wait in ignorance until an incident occurs or is detected. An example of such crimes being people masquerading as celebrities in social networking sites e.g. Facebook to cause harm especially minors. In other instances, most computer crime perpetrators have been successful when the security infrastructure of the host organisation is not robust, hence can easily be compromised if persistent attacks are launched at it.

According to myjoyonline.com (2012), nowadays criminals are using ICT to break into peoples bank accounts, withdraw money from peoples account on the blind side of the police. To this, The Ghana Police Service says they are exploring modern technology to combat crime. Director-General in charge of Research, Planning and ICT, David Asante-Apeatu, believes this is crucial in ensuring citizens get adequate protection. He says the service has acquired some equipment to facilitate the work of personnel, and also improve their safety in the line of duty. The Police Administration is taking steps to avert the situation where

criminals outwit security agencies in future, with ICT training at the centre of its strategies, he said. The Police Administration agreed that the service lack modern ICT equipment and qualified IT personnel that thirty-four officers selected from across the country have been undergoing trainer of trainers ICT programme by the Ghana Investment Fund for Electronic Communications as criminals in the world over have always been a step ahead of security agencies.

Director-General in charge of Research, Planning and ICT, David Asante-Apeatu, however indicated that the Police Service is committed in its resolve to scale the challenge, with new gadgets. They include Automated Fingerprint Identification System, walkie-talkies, and the establishment of forensic laboratories at all regional commands. “It (crime combat) has been a challenge both in Ghana and elsewhere but we are on top of issues. We have made an ambitious step in making sure we have computerized our stores, our record office and our pay roll integrating all these units into one system”. According to Mr. Asante-Apeatu, there are efforts to computerize police road checks by introducing a system where police can have on-the-spot information on vehicles. “When it comes to DVLA for example, very soon police are going to come out with a system whereby police can easily access information on drivers’ license and vehicles (myjoyonline.com, 2012).

Abor (2004) also reported that the developments of ICT have radically changed the way organizations in Ghana do business. Technological innovation has transformed the Ghanaian economy, especially the financial industry; as many banks are making huge investments in technology to maintain and upgrade their infrastructure, in order to provide new electronic information-based services. However, innovations in strategic decision-making for organizations in Ghana have been slow and very few institutions in Ghana have adopted Business Intelligence systems to enhance decision-making.

According to Gottschalk (2010), Computer systems have allowed criminal activities to thrive in financial institutions due to the rapid advances in technology and globalization of the financial industry. Criminals are able to transfer large sums of monies from banks through wired systems and various technologies such illegal activities.

A review of the literature portrays a paucity of research that explores such crimes in African and for that matter, Ghanaian settings. This position paper highlights some of such computer crimes from the international literature with a major focus on the types that can potentially occur. The awareness of such potential crimes and how they can be perpetrated can inform management decision making in strategies that can be adopted to mitigate the potential incidences of such computer crimes. Charney and Alexander (2001) are of the view that the importance of security and security controls as the tools to tackle computer crimes are usually facilitated by insiders who divulge password or confidential information that aid criminals in carrying out their activities. It is our opinion that it is important for computer crimes to be properly investigated as history resonates with evidence that criminals will frequently abuse new technologies to benefit themselves or injure others (Charney and Alexander, 2001).

2.5 Implications of computer crimes for organisational management

Management of most financial organizations often do not realize the value of prevention in the area of computer security, but wait in ignorance until an incident occurs or is detected (Prasad, Kathawala, Bocker & Sprague, 2003). Wang and Huang (2011), report that concern about computer crime is being fuelled by increased media reports (such as the WikkiLeaks) that reveal the sheer number of intrusions and the damage being caused. Furthermore, the advent of the personal computer has greatly affected the outlook toward computer crimes. Aaland (as cited by Prasad, Kathawala, Bocker and Sprague, 2003) observed that now with

35 to 40 million PCs in the work place, organisations large and small alike are vulnerable to computer crimes.

According to Chawki (2009), the rapid evolution of information technology, the proliferation of computer and media devices and the rapid growth in the use ICT and the internet for organisational management have spawned new forms of crimes and made old crimes easier to commit. Computer crimes like cyber-stalking; identity theft; pornography; fraud; scams; copyright violations, hacking and creating malicious code are some of the incidences that have been triggered by this rapid growth (Chawki, 2009). Other examples of computer crimes include people masquerading as celebrities in social networking sites, for example, Facebook to cause harm especially to the minors. In other instances, most computer crime perpetrators have been successful when the security infrastructure of the host organisation is not robust, hence can easily be compromised if persistent attacks are launched at it (Chawki, 2009). In view of the complexities in computer crimes that can occur, there is the need for awareness to be created about some of the potential crimes that can be perpetrated in organisations such as the university.

2.6 The Impact of ICTs on Information Gathering and Security Management

Information and communication technologies have swept the world with powerful force, thereby affecting the society in various ways. In this regard, Folarin (2009) notes that technology is equipment that the user uses to interact with people. With this, Dugo (2008) posits that in the past few decades' information and communication technologies have transformed in all spheres of life. Its potential for reducing manual operation (the search for sources) in fostering the media has increased rapidly.

The role of information has also been stressed in security management. Zack (2009) posits that, to nip any evil plan in the bud, information about such intent must be available so as to map out strategies to prevent the occurrence. That, even when these crisis, disasters or chaos occurred in the society, accurate and timely information always help to proffer solution to ameliorate the situation. When it comes to information, Zack (2009) stresses that the internet has it all. That, there is more information on computers and other ICTs than one could ever possibly digest. The greatest thing about the web is that "you can use it to keep in touch with changes in the field and groups that make these changes happen". Zack (2009) explains that by using the search engines, you can even learn about the internet itself or about a piece of ICTs equipment introduced into your office. "You have the choice to download information about the equipment or print out pages for study, demonstration and information on how you can procure one". Zack (2009) concluded that in this modern world everybody has to be ICTs compliance so as to help in providing information and constructive suggestions on how to combat terrorism and other security challenges that threaten the existence of our society.

Muhammed–Nasiru and Kasimu (2012) posit that ICT can serve as surveillance and when it is well established craft involving technique and better gadgets aid information gathering and security management. However, most surveillance has physical and electronic aspects and is preceded by reconnaissance and not infrequently by surreptitious entry (to plant a monitoring device).

Today, in addition to anticrime advertising, case processing using media technology, and police surveillance systems based on the older technologies of audio- and videotaping, there is an abundance of newer media technologies capable of both facilitating and constraining communication, interaction and realization of fluid identities (Greer, 2010). Moreover, the digitized, computerized, and networked information and communication technologies

exemplified by the internet have created virtual worlds with their own changing norms, value and codes of practice. Altering the ways in which "people engage in time and space" (Greer, 2010) However, the idea of using surveillance for the purpose of information gathering and security management received a boost with the advent of internet computer. According to Surette (2007), these technological transformations have created new opportunities and risks for crime and victimization, and for surveillance and crime control. For example, close circuit television cameras, information gathering, and data processing have transformed how people perceive and negotiate their social worlds with caution and reserve.

Muhammed–Nasiru and Kasimu (2012) added that in addition to improving the quick delivery of information and security management, computer and telecommunication technology can improve both the quality and quantity of information reported. Technology enables the existing news industry and security agencies to deliver its news and findings in real time, and largely increased the quantity of information that can be made available.

Lachlan (2004) in related view stated that most media imagery and video are recorded from a perspective on or near the earth, "recent years have seen the growth of imagery and video of the earth but observed from hundreds of miles above the ground". Remote- censoring satellite imagery has since the end of the cold war, grown dramatically to become an almost daily path of media content. On the Web; members of the public can type their address and see a satellite image taken of their neighbourhood. Satellite imagery not only plays an important role in security and military operation, it can also be invaluable for journalists covering story on the environment or the influence of development on farm land, for example. Looking at weather patterns over time can also provide vital information and help people to prepare for severe weather (Lachlan, 2004).

2.7 ICT Surveillance and the Law of Invasion of Privacy

According to Muhammed–Nasiru and Kasimu (2012), despite the fact that surveillance, information and communication technologies serve as tools for information gathering and security management, it is apparent that the employment of CCTV cameras seems to be a direct invasion of privacy. Though, it may be argued that surveillance is in public and government interest, and as well serves as the first step towards a submissive and controlled society, the fact that the general public has the right to privacy even in public area should not be undermined.

In his view, Nieto (1997) asserts that video surveillance is analogous to mechanical police officer. He added: It does not intrude upon an individual sphere of privacy, but rather records events occurring in public space for which individuals do not have reasonable expectations of privacy. Commenting on this, Rosen (2004), states that CCTV cameras have a mysterious knack for justifying themselves regardless of what happens to crime. He wrote: When crime goes up, the cameras get credit for detecting it, and when crime goes down, they get the credit for preventing it. However, the nagging questions are; which condition may warrant public surveillance? What are the association legal and constitutional implications? And how effective are information and communication technologies for information gathering and security management? With regard to privacy right, section 37 of the 1999 Constitution of the Federal Republic of Nigeria made provisions guaranteeing the privacy of the citizen of the country in his home, correspondence, telephone conversation and telegraphic communication.

In view of this, Obaze and Fashamu (2006) avers that a lot of arguments have also been raised on the necessity of privacy laws, if information must be gathered and published for and in the interest of the public.

2.8 The Significance of ICTs on Information Gathering and Security Management

For effective information gathering and security management (Gharoro and Igbafe, 2000) observed that, government agencies use computer for a wide range of purposes. These include but not limited to accounting, budgeting, forecasting, storage of information on birth, death, social welfare, census and population data, voting registers, among others.

Today, unprecedented information are being gathered through effective surveillance with the aid of satellite and other technological gadgets. Surveillance, according to (Muhammed–Nasiru and Kasimu, 2012) when examined critically, has much in common with investigative reporting. It is a fact that this will go a long to enhance effective security management in any human organisation.

However, people who may be involved in the act of information gathering and security management must indeed possess the following qualities. This include sound event analysis, sense of public interest, research, analytical and good communication skills, a mind for adventure, capacity to make sound and balanced socio-political judgments. More so, the security management must be courage, ability to see the event behind the event, knowledge of photo journalism, computer literate and above all ICTs compliance.

2.9 Summary

Information and communication technologies (ICTs) as tools for combating financial crime information and gathering and security management remain a vital aspect of our life. It is important to note that at the federal, state, local government and even in remote areas, security management has become an issue of national and international concern. The contribution of surveillance and ICT in security management goes beyond the comprehension of the ordinary man on the street. However, at this critical stage of national life, where

insecurity of lives and properties remain as issue of worry and where people now live with uncertainty and fear, where they are forced to sleep with one eye open, the employment of surveillance and technology seems vital.

If information technologies (ICTs) are properly managed, the current problems of corruption in Ghana can be reduced drastically. This will be achieved with the usage of effective computer connectivity (Internet) and employment of well trained service personnel to enhance their effective use. To this end, Nwabuze (2005) presents a clear picture of the above, when he states that the internet can be seen as an inter-connectivity of computers and some other devices like mobile phones, which exchange information with the aid of telephone lines; The computers and other communication gadgets are in a kind of network which permits or facilitates communication among them.

It is worthy to note that, the Internet is one of the most prominent factors that gave credibility to the statement that the world is a global village. By and large, financial crime when matched effectively with ICT, information gathering and security management, will be very easy and this will go a long way to bring about peace and development in our society. Therefore, the Governments should henceforth continue to mount or place CCTV at every strategic position across the country if possible. Not just to mount this communication gadgets, but to be complemented with appropriate training of personnel for their effective use.

In addition, every member of the society should see himself/herself as a security agent working with the government authority in combating crimes and ensuring security of lives and property.

REFERENCES

Aidoo, D. B., Akotoye, F.X.K., & Ayebi-Arthur, K. (2012). 'Academic 419': Locating computer crimes in the use of ICT for the management of educational systems in Ghana – The case of University of Cape Coast. *Journal of Educational Management*, 6: 102-111.

BiztechAfrica (2011). *Ghana to curb cyber crime*. Retrieved November 30, 2013, from http://www.biztechafrica.com/article/ghana-moves-curb-cyber-crime/1533/

Bureau of Justice Assistance, (2009). *Internet Crime report, Internet Crime complaint centre, Bureau of Justice Assistance, US Department of Justice*, http://www.ic3.gov/media/annualreport/2009 _IC3Report.pdf, 2013.

Citifmonline (2011). *Ghana among top 10 on global internet fraud table*. Availabe at http://www.citifmonline.com/index.php?id=1.287156.1.420460 Jun 10.

Chawki, M. (2009). *A Critical Look at the Regulation of Cybercrime*. Retrieved on November 30, 2011 from http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2009_1/chawki/chawki.pdf

Daily Guide (2013). Fight financial crime through vigilance. *Business News of Wednesday*, 23 October 2013 Retrieved on 06/12/2013 from http://www.ghanaweb.com/GhanaHomePage/NewsArchive/artikel.php?ID=289684

Dugo, H (2008). *Journalists Appropriation of ICTs in News Gathering and Processing*. Rhodes University.

BOSWORTH, B.P. and TRIPLETT, J.E. (2000). *What's new about the New Economy? It, Economic Growth and Productivity'*, Brookings Economic Papers, October 20.

Ghana Business News (2009). *Ghana Business News Cyber crime: Giving a bad name to Ghana February 17*. Retrieved on 20/11/2013from http://www.ghanabusinessnews.com/2009/02/17/cyber-crime-giving-a-bad-name-to-ghana/

Gharoro, EP, Igbafe, A.A. (2000). Pattern of drug use amongst antenatal patients in Benin City. *Nigeria. Med Sci Monit*, 6 (1): 84–87.

Greer, C. (2010). *Crime and Media***:** A Reader. London: Routledge.

Gee, G. and Kim, P. (2011). *Doppelganger Domains.* Retrieved 15 September from files.godaigroup.net/doppelganger/Doppelganger.Domains.pdf

Ibezimako, M. (2006). Information and Communication Technologist (ICTs) in Modern Public Relations Practice: Uses, Impact: in Mass Media Review. *An International Journal of Mass Communication*, p.84.

Idogho and Ogedegbe (2010). The Role of ICT in Poverty Reduction in Nigeria. *The Journal of Arts, Management Science and ETF Project*.

Kabay, M.E. (2008). *Computer Security Handbook*, 5th ed. New York: John and Wiley.

Lachlan, K. (2004). *Introduction to Mass Media*. United States of American: Kendall / Hunt Publishing Company.

Muhammed–Nasiru, I. and Kasimu, S. (2012). *Surveillance, Information and Communication Technologies (ICTS) as tools for information gathering and security management department of mass communication, school of information and communication technology (ICT),* Auchi polytechnic, Auchi.

Nieto, M. (1997). *Public Video Surveillance: Is it an Effective Crime Prevention Tool*?

Nwabueze, C. (2005). *The Art of Investigative Reporting: A Practical Guide*. Enugu: Daisy Press.

Nwosu, I. (2004). *Digital Public Relations Concept and Practice. In J. Nkwocha (Ed). Digital Public Relations*. Lagos: Zoom len Publishers.

Oak, M. (2009). *Intelligent Life on the Web*. Retrieved 09/01/2013 September from http://www.buzzle.com/articles/types-of-computer-crimes.html

Obaze, A and Fashanu, F (2006). *Mass Communication Law and Ethics*. Ibadan: Safmos Publishers.

Okpoko, J. (2009). *Understanding International Communication*. Zaria: University Press Limited.

Prasad, J.N., Kathawala, Y., Bocker, H.J. & Sprague, D. (2003). The Global Problem of Computer Crimes and the Need for Security. *Industrial Management*, 24-28.

Rao, K.G. and S. Dey (2012). An intelligent decision making architecture for banks: Business intelligence and knowledge management systems integration. *J. Econ. Develop. Manag. IT*, 4(1): 49-63.

Rollins, J., Wyler, S. L. (2010). *International Terrorism and Transnational Crime: Security Threats, U.S. Policy, and Considerations for Congress*. Retrieved December 15, 2013 from http://www.fas.org/sgp/crs/terror/R41004.pdf

Rosen, J (2004). *The Naked crowd*: *Reclaiming security and Freedom in an Anxious Age*. New York: Random House.

Salwan, D. (2008). *Business intelligence in financial institutions. Proceedings of the 2nd National Conference*, IndiaCom. New Delhi, India: JAY Publishers.

Schneider, F.; Enste, D.H. (2000). Shadow Economies: Size, Causes, and Consequences. *Journal of Economic Literature*, 38: 77-114

Saunders, K. and Zucker, B. (1999). Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act', in Wall, D. (ed), special issue on E-Commerce. *International Review of Law, Computers and Technology*, vol.13, no. 2

Surette, R. (2007). *Media, Crime and Criminal Justice: Images, Realities and Policies*, 3rd ed. Belmont, CA: Thomson Wadsworth.

Taylor, D. (2012). *The Literature Review: A Few Tips on Conducting It*. Retrieved on 17/12/2013 from www.writing.utoronto.ca

Telecoms, Internet and Broadcast in Africa (2007). *Telecoms, Internet and Broadcast in Africa Issue no 349 8th April 2007 POLICE ADVOCATE FOR LAWS TO COMBAT CYBER FRAUD IN GHANA.* Retrieved 10 October from http://www.balancingact-africa.com/news/en/issue-no-349/computing/police-advocate-for/en

UNDP (2001). *United Nations Development Programme (UNDP), United Nations Office on Drugs and Crime (UNODC): Corruption. A crime against...* Retrieved on 17/12/2013 from www.yournocounts.org

Wang, S.Y.K. and Huang, W. (2011). *The Evolutional, the types of identity thefts and online frauds in the Era of Internet*. Journal of Criminology Retrieved on November 12, 2013 from http://www.internetjournalofcriminology.com/Wang_Huang_The_Evolutional_View_of_the_Types_of_Identity_Thefts_and_Online_Frauds_in_the_Era_of_Internet_IJC_Oct_2011.pd

Zack, R. (2009). *Information and Communication Revolution in the 21st Century*. Lagos: Prime Target Venture.

Zetter, K. (2010). *Sarah Palin E-mail Hacker Sentenced to 1 Year in Custody.* Retrieved 02, November 2011 from http://www.wired.com/threatlevel/2010/11/palin-hacker-sentenced/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+wired27b+%28Blog+-+27B+Stroke+6+%28Threat+Level%29%2

CHAPTER THREE

METHODOLOGY

3.1. Introduction

The main importance of research is to produce knowledge that can be applied outside a research setting. Research also forms the foundation of programme development and policies everywhere around the universe. It also solves particular existing problems of concern. According to Creswell (2003), research methodology refers to the method adopted in carrying out a research. Research methodology is a collective term for the structured process of conducting research. The term research methodology referred to a method that compasses the procedure followed to analyse and interpret the data gathered.

There are many different methods used in various types of research and research as a term is usually considered to include research design, data gathering and data analysis. Research methodology can be quantitative (for example, measuring the number of times someone does something under certain conditions) or qualitative (for example, asking people how they feel about a certain situation). Research methods are generally used in academic research to test hypothesis or theories. In the developed world, research methods are employed to gather data/information for various purposes including feasibilities studies, planning, monitoring and evaluation (Tabiri, 2012).

The methodology for this study was treated under research design, selection of case, selection of subjects (population, sample size, sampling technique), and instrumentation, mode of data collection, method of data analysis and presentation of results.

3.2 Research Design

A quantitative research approach was used in this study. According to Dawson (2009), quantitative research generates statistics through the use of large-scale survey research, using methods such as questionnaires or structured interviews. The research method used was self-administered questionnaires. The research also employed a cross-sectional design. According to Bryman and Bell (2007), research designs are classified as experimental, cross-sectional, longitudinal, case study and comparative. Cross-sectional research design involves a collection of quantitative data. It is suited for research that involves looking into a phenomenon, for example, a technology, at a particular time from different perspectives. Business Intelligence concerns a technological phenomenon, a cross-sectional research design was therefore considered appropriate for the study. The purpose of the study suggests that it is both exploratory and descriptive. Research involves three kinds: exploratory, descriptive and explanatory. Exploratory is valuable when the research is to study a new area and/or test methods, such as surveys and survey questions, for investigating that area. A descriptive study is used when an issue needs to be explained in more detail. Surveys rely on description and involve questioning individuals on topics and then describing their responses (Jackson, 2011). The strategy used in this research was that of a survey, as surveys often test results, self-completion questionnaires and attitude scales. A survey is used to scan a wide field of issues, in order to measure or describe any generalized features.

Crossman (2013) described quantitative research as a research that uses numerical analysis. In essence, this approach reduces the data into numbers. The researcher knows in advance what he/she is looking for and all aspects of the study are carefully designed before the data is collected. The objective of quantitative research is to develop and employ mathematical models, theories and/or hypotheses pertaining to phenomena.

Anderson and Taylor (2009) added that quantitative research is generally done using scientific methods, which includes the following steps:

- Developing models, theories, and hypotheses of what the researcher expects to find.
- Developing instruments and methods for measuring the data.
- Experimental control and manipulation of variables.
- Collecting the data.
- Modeling and analyzing the data.
- Evaluating the results.

The greatest strength of quantitative research is that it produces quantifiable, reliable data that are usually generalizable to some larger population. Quantitative analysis also allows researchers to test specific hypotheses, in contrast to qualitative research, which is more exploratory (Anderson and Taylor, 2009).

The greatest weakness of the quantitative approach is that it decontextualizes human behaviour in a way that removes the event from its real world setting and ignores the effects of variables that have not been included in the model. It also lacks a depth and richness of data that is present with qualitative research. Because there are so many participants using quantitative methods, it is impossible to know the details about each and every one (Anderson and Taylor, 2009).

3.3 Selection of Case

Ghana Police Service Commercial Crime Unit was the case to be investigated and the justification for the selection was that it is located in the Headquarters of the Ghana Police Service. The reason being that, this unit use ICT as a tool to combat financial crime in the country.

3.4 Selection of Subjects

3.4.1 Population

In the Commercial Crime Unit of Ghana Police Service were 46 personnel who were in charge of all the ICT facilities of the service.

According to Creswell (2003), population is the units for which information is required. Creswell (2003) further explained that population is any set of persons or objects that possesses at least one common characteristic. Evaluating the prospects and challenges of ICT in combating financial crime, this study sampled the views of 38 ICT personnel at the headquarters of Commercial Crime Unit and generalized it to the entire population of the police service. For the purpose of the study, questionnaire was administered to all of them.

3.5 Instrumentation

Instrumentation used for this study was questionnaire. According to Fraenkel and Wallen (2000), instrumentation is generally the whole process of collecting data. It involves not only the selection or design of the instrument but also the condition under which the instrument will be administered and the most common type of instrument used in survey research is the questionnaire. To Ivancevich (2004), the use of questionnaire is usually the least costly for collecting information. It is an effective way to collect a large amount of information in a short period. There are several ways to administer questionnaires and data are usually collected through the use of questionnaires, although sometimes researchers directly interview subjects.

According to Kumar (2005), the questionnaire method is economical in terms of effort, since a single copy can be duplicated and distributed to numerous respondents to generate a large

amount of data for the study. Questionnaire also provides access to more respondents that are educated and gives an opportunity for respondents to give frank and anonymous answers. The questionnaire method gives a high response rate.

A questionnaire is a list of written questions that can be completed in one or two basic ways. Firstly, respondents could be asked to complete the questionnaire with the researcher not present. This is a postal questionnaire and (loosely) refers to any questionnaire that a respondent completes without the aid of the researcher. Secondly, respondents could be asked to complete the questionnaire by verbally responding to questions in the presence of the researcher.

Questionnaires are restricted to two basic types of questions: Close-ended question (or "closed question") is a question for which a researcher provides a suitable list of responses (e.g. Yes / No). This produces mainly quantitative data. Open-ended question (or "open question") is a question where the researcher doesn't provide the respondent with a set answer from which to choose. Rather, the respondent is asked to answer "in their own words". This produces mainly qualitative data. It must be pointed out that questionnaires have their own limitations which include time consuming, language barrier and lack of opportunity for probing responses. The study addressed these limitations by making the questionnaire open-ended, interpreting questionnaires to farmers in the local dialect (bono) and tacking transect walk among others in the study area.

The questionnaire was itemised under the following subheadings: Bio data of the respondents, availability and adequacy of ICT facilities for combating financial crime, type and level of financial crime in Ghana, competency for financial crime combat, challenges in using the ICT for combating financial crime and general comments. See Appendix A for questionnaire.

3.6 Pre-Testing

The researcher tested the questionnaire on some selected police personnel in the commercial crime unit office, headquarters to see the weakness of the question. Based on the answers provided by the respondents, changes and amendments were made to the questionnaires.

Bell (2005), have advised that "however pressed for time you are, do your best to give the questionnaire a trial run. Because without a trial run, there is no way of knowing that the questionnaire will succeed. According to Kumar (2005) pre-testing fulfils the role of a dress rehearsal and is useful for the following reasons: to detect the main flaws, pre-formulate questions, illustrate kind of data which will result from the main study. It was based upon these reasons that the researcher after deciding on the research strategy thought it prudent to try out the technique chosen as the main data collection device.

3.7 Mode of Data Collection

The researcher administered the questionnaires to all the 38 service personnel in their respective office and laboratories. Completed questionnaires were collected there and then.

3.8 Method of Data Analysis and Presentation of Results

After retrieving the questionnaires administered, correctly completed ones were selected and uncompleted/spoiled ones were rejected. Consistency in responses was checked and a coding manual was designed to translate the categorical responses to numbers to facilitate the analysis of data. Statistical Package for Social Sciences (SPSS) was used to enable the researcher draw inferences, meanings, analysis and conclusions from the data collected.

According to Healey (1993), the Statistical Package for Social Sciences (SPSS) is the most widely used statistical software in the social sciences. Statistical methods like simple frequencies, percentages, and cross tabulations was used to present the results of the study.

3.9 Ethical Considerations

The researcher sent an introductory letter seeking permission to conduct the research which involved Ghana Police Service, Commercial Crime Unit from the Department of Information Studies, University of Ghana to the Crime Officer of Commercial Crime Unit, Headquarters, Accra. Neuman (2007) of the view that a fundamental ethical principle of social research is: never coerce anyone into participating; participation must be voluntary at all times. Permission alone is not enough; people need to know what they are being asked to participant in so that they can make an informed decision. Neuman (2007) further stressed that the law and codes of ethics recognise some clear prohibitions: Never cause unnecessary or irreversible harm to subjects; secure prior voluntary consent when possible; and never unnecessarily humiliate, degrade, or release harmful information about specific individuals that was collected for research purposes. In other words, you should always show respect for the research participant.

The researcher explained the rationale behind the study and as service personnel was able to explain almost everything in the questionnaire to the respondents in the service language. Respondents have the right to withdraw from the study at anytime.

According to Neuman (2007), survey researchers invade a person's privacy when they probe into beliefs, backgrounds, and behaviours in a way that reveals intimate private details. Ethically, researchers protect privacy by not disclosing a participant's identity after

information is gathered. This takes two forms both of which require separating an individual's identity from his or her responses: anonymity and confidentiality.

According to Neuman (2007) anonymity means that, people remain anonymous or nameless by protecting the identity of specific individuals from being known. For example, by providing a social picture of a particular individual, but gives a fictitious name and location. He continues that, even if a researcher cannot protect anonymity, he or she always should protect participant confidentiality. Confidentiality can include information with participant names attached, but the researcher holds it in confidence or keeps it secret from the public disclosure. Privacy, anonymity and confidentiality of the respondents were assured by the researcher and her team.

REFERENCES

Anderson, M.L. and Taylor, H.F. (2009). *Sociology: The Essentials*. Belmont, CA: Thomson Wadsworth.

Bell, J. (2005). *Doing Your Research Project.* 4th ed., Buckingham: Open University Press, p.52.

Bryman, A. And Bell, E. (2007). *Business Research Methods* 2nd ed. Oxford: Oxford University Press.

Crossman, A. (2013). *An Overview of quantitative research methods: surveys, secondary data, and experiments*. Retrieved on 02/12/2013 from http://sociology.about.com/od/Research/a/Overview-Of-Quantitative-Research-Methods.htm

Creswell, J. (2003). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches* 2nd ed., London: SAGE Publications, p. 29.

Fraenkel, J. R. and Wallen, N. E. (2000). *How to Design and Evaluate Research in Education* 4th ed., New York: McGraw–Hill, p.101.

Healey, F. J. (1993). *Statistics: A Tool for Social Research* 3rd ed., Belmont: Wadsworth. p.72.

Ivancevich, J.M. (2004). *Human Resource Management*. New York: McGraw –Hill. p. 165.

Kumar, R. (2005). *Research Methodology: a Step-by-Step Guide to Beginners* 2nd ed., London: SAGE Publications, p.126.

Neuman, W. L. (2007). *Basics of Social Research: Qualitative and Quantitative Approaches* 2nd ed., New York: Pearson Education Inc.

Tabiri, C. (2012). *ICT and the Provision of Agricultural Information for Cashew Farmers in Ghana: A Case Study of Techiman in the Brong Ahafo Region*. M PHIL thesis, Department of Information Studies, University of Ghana.

CHAPTER FOUR

DATA ANALYSIS AND PRESENTATION OF FINDINGS

4.1 Introduction

This chapter focuses on the analysis of data collected through the use of questionnaires. Data was analyzed in relation to the objectives of the study as the results of the analysis have been presented in tables showing frequencies, percentages and figures of responses given by the respondents who are personnel of the Ghana Police Service under study. The discussion relates to the findings of the study, to the literature review and Mwakalinga and Kowalski's adaptive information security systems model which served as the theoretical framework of the study. The response rate was (82%) as 46 questionnaires were administered and 38 were retrieved.

The chapter has been presented under the following sub-headings:

1. Background information of the respondents under study
2. Availability and adequacy of ICT facilities for combating financial crime
3. Competency for financial crime combat
4. Challenges in using the ICT for combating financial crime
5. Suggestions for improvement of the use of ICT in combating financial crime in Ghana.

Descriptive research was employed using simple descriptive statistics to test for differences between groups.

4.2 Background information of respondents of private universities

Data was gathered on the background information of the respondents under study in order to determine its influence on their ability to use ICT in combating financial crime. The background information included age, gender, educational level, rank, and number of years in the service.

4.2.1 Age distribution of the respondents

Age is of importance as it has a bearing on the ability of staff to adapt, accept and implement change in their service delivery. From the table 4.1, it can be observed that majority of the respondents representing 47.4% fall between the ages of 36-45, whereas 23.7% fall between 31-35 years, 10.5% respectively were between 26-30 and 46-55 years, and 7.9% fall below 25 years. From the findings, it can be said that the respondents were in the active working age. This age pattern suggests that majority of the respondents had matured emotionally and therefore gained enough experience to be able to adapt to change in service delivery.

Table 4.1 Age distribution of respondents

Age of respondents	Frequency	Percent
Below 25 years	3	7.9
26-30 years	4	10.5
31-35 years	9	23.7
36-45 years	18	47.4
46-55 years	4	10.5
Total	38	100.0

Source: Field Data, 2013

4.2.2 Gender of respondents under study

Data on the gender of the respondents reveals that 63.2% of the respondents were males and 36.8% percent females. The implication here is that the males were more than the female as at the time of study.

4.2.3 Highest Educational level of the respondents

Highest educational level was sought to determine whether the personnel in the police service have the capacity of using ICT in combating financial crime. From the analysis it was revealed that most 36.8% of the respondents have attained first degree, 21.1% had attained Master degree, whilst the rest of the respondents had attained SSSCE, O' level and A' level. From the findings, it can be deduced that all the respondents in the Police Service have some form of educational background which can help in ICT usage. Table 4.2 depicts the level of education of respondents.

Table 4.2 Highest Educational level of the respondents

Educational level	Frequency	Percent
O' Level	5	13.2
A' Level	4	10.5
SSSCE	7	18.4
First degree	14	36.8
Master degree	8	21.1
Total	38	100.0

Source: Field Data, 2013

4.2.4 Rank of Respondents

Table 4.3 shows the ranks of the respondents. Among ranks that answered the questions for the study were: ACP (2.6%), C/Superintendent (2.6%), ASP (7.9%), Chief Inspector (5.3%), Inspector (7.9%), Sergeant (28.9%), Corporal (21.1%), Lance Corporal (15.8%) and Constable II (7.9%). The implication of these ranks to the study is that the higher the rank the more knowledge one can have on the job and this researcher believed that with these ranks applying ICT technologies into financial crime combating will not be a problem.

Table 4.3 Rank of the respondents

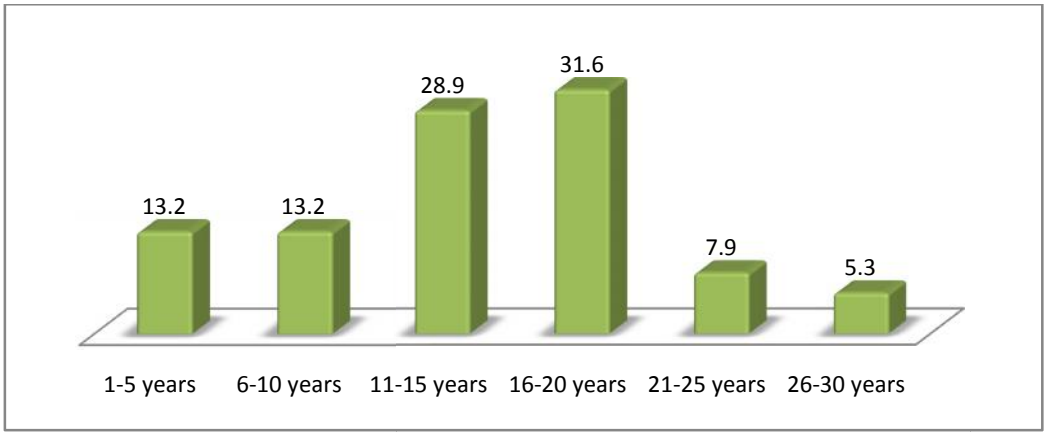
Rank	Frequency	Percent
Constable II	3	7.9
Lance Corporal	6	15.8
Corporal	8	21.1
Sergeant	11	28.9
Inspector	3	7.9
Chief Inspector	2	5.3
ASP	3	7.9
C/Superintendent	1	2.6
ACP	1	2.6
Total	38	100.0

Source: Field Data, 2013

4.2.5 Number of years in the services

Number of years in services was sought to determine whether the year's one serve can equip him/her for the use of ICT in combating financial crime. Figure 4.1 below depicts the responses received on the number of years respondents were in services.

Figure 4.1 Number of years in the services



Source: Field Data, 2013.

From Figure 4.1, 31.6 % of the respondents indicated that they have been in the services for 16-20 years, 28.9% were in the service for 11-15 years, 13.2% of the respondents indicated

that they were in the service for 6-10 and 1-5 years respectively. The remaining respondents 7.9% indicated they were in the service for 21-25 years whilst 5.3% of the respondents also indicated that they were in the service for 26-30 years. From the data, it can be deduced that majority of the respondents have been in the service for long period of time and this can beneficial.

4.3 Availability and Adequacy of ICT facilities for Combating Financial Crime

The first objective of the study was to determine whether the Commercial Crime Unit of Ghana Police Service has enough ICT facilities for combating financial crime. According to Susan et al, (2013), combating financial crime require sufficient and availability of ICT facilities to perform their duties effectively. Without these resources it will be very difficult for the police to communicate, respond to citizens' distress calls, and move from one place to another in response to criminal activities. Susan et al, (2013) further explained that availability of ICT facilities and other resources motivates the officers to continuously perform their duties according to the expectations of stakeholders. Specifically the officers require modern technology and training on the use of the same. To arrive at the answer, question was posed to the respondents that effect. The results in Table 4.4 show the available, status and usage of the ICT facilities available to the Ghana Police Service.

Table 4.4 ICT facilities available for GPS

ICT facilities	Available		Status		Usage	
	Yes	No	Working	Not working	Being used	Not being used
Mobile networks software	10(26.3%)	-	19(50%)	-	9(23.7%)	-
Mobile communication devices	12(31.6%)	-	16(42.1%)	-	10(26.3 %)	-
Biometric scanner	-	15(39.5 %)	-	6(15.8%)	-	17(44.7 %)
PC tracking system	-	18(47.4 %)	-	-	20(52.6 %)	-
Retinal scanner	-	23(60.5 %)	-	-	-	15(39.5 %)
Fingerprint scanner	18(47.4%)	-	-	15(39.5%)	5(13.2%)	-
Voice biometrics	-	31(81.6 %)	-	-	-	7(18.4 %)
Automated fingerprint identification system	13(34.2%)	-	22(57.9%)		3(7.9%)	-
Walkie-talkie	15(39.5%)	-	12(31.6%)	-	11(28.9 %)	-
Intrusion detection system software	-	24(63.2 %)	-	6(15.8%)	-	8(21.1 %)
Video cameras	20(52.3%)	-	-	9(23.7%)	9(23.7%)	-
Forensic acoustics	18(47.4%)		12(31.6%)	-	8(21.1%)	-

Source: Field Data, 2013

From Table 4.4, it can be observed that the GPS have mobile networks software, mobile communication devices, fingerprint scanner, automated fingerprint identification system, Walkie-talkie, video cameras, and forensic acoustics were available, working and were being used in operations for financial crime combating as respondents have indicated in the Table 4.4. Respondents also indicated there are some of the ICT facilities which were not available. These includes biometric scanner, PC tracking system, retinal scanner, voice biometrics and intrusion detection system software as respondents have indicated with their frequency and percentage respectively in the table. From the analysis it can be said that Ghana Police Service lack the necessary ICT facilities.

Table 4.5 Level of adequacy of the ICT facilities for combating financial crimes

Level of adequacy of the ICT facilities	Very low	Low	Moderate	High	Very high
ICT facilities	12(31.6%)	7(18.4%)	10(26.3%)	5(13.2%)	4(10.5%)
Software	18(47.4%)	9(23.7%)	8(21.1%)	-	3(7.9%)
Hardware	28(73.7%)	10(26.3%)	-	-	-
Personnel	5(13.2%)	-	15(39.5%)	8(21.1%)	10(26.3%)
Skills support	8(21.1%)	-	21(55.3%)	9(23.7%)	-

Source: Field Data, 2013

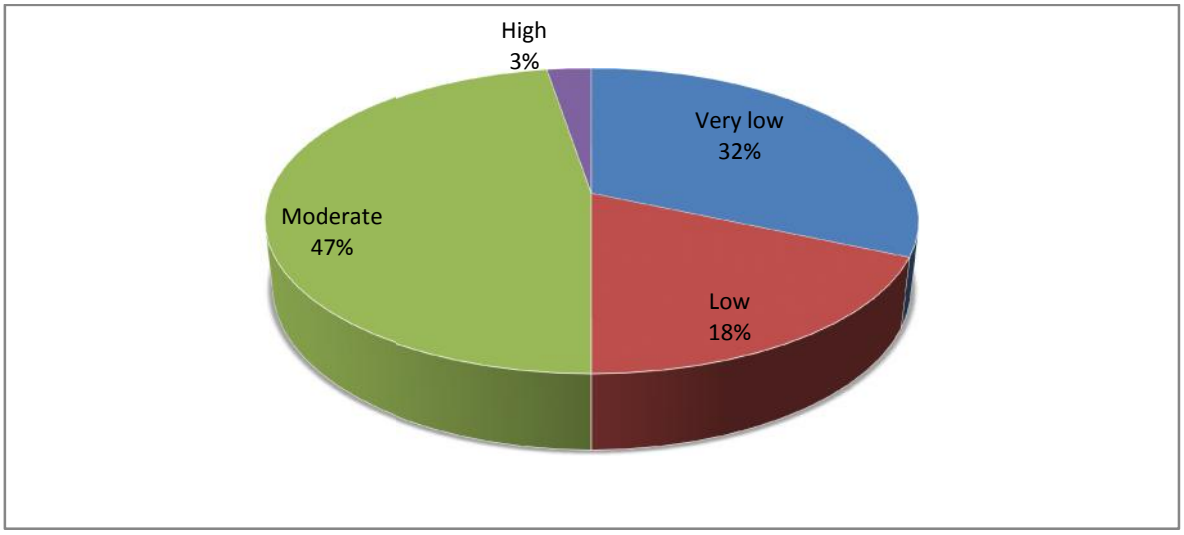
A question was inquired on the respondents' level of adequacy of the ICT facilities for combating financial crimes. With this the results clearly show that, ICT facilities for combating financial crime were not adequate. The results indicate that 12 (31.6%) respondents out of the total respondents of 38 rate the ICT facilities very low, 7 (18.4%) rate

the ICT facilities as low, 10 (26.3%) rate it as moderate, that ICT facilities for financial crime combating was very low, 10 (26.3%) – moderate, 5 (13.2%) of the respondents rate the ICT facilities available to GPS as high while 4(10.5%) rate it as very high. With the software adequacy 18 (47.4%) rate it as very low, 9 (23.7%) rate ICT adequacy as low, 8 (21.1%) rate it as moderate whiles 3 (7.9%) rate it as very high. For hardware majority 28 (73.7%) rate it as very low whilst the remaining respondents rate the ICT adequacy in the Ghana Police Service as low. Concerning the personnel, 15 (39.5%) rate it as moderate, 10 (26.3%) rate it as very high, 8 (21.1%) – high whilst 5 (13.2%) of the respondents rate its adequacy as very low in the area of ICT facilities to the Ghana Police Service. To skills support, majority 21 (55.3%) rated as moderate, 9 (23.7%) rate it as high whilst 8 (21.1%) of the respondents rate it as very low. From the findings it can be said that the Level of adequacy of the ICT facilities for combating financial crimes were not to the modern ICT age.

4.3.1 Quality of availability of ICTs facilities for combating financial crime

It was expected that in the era of ICT, Ghana Police Service should have the best quality of ICT facilities in combating financial crime. The results concerning quality of availability of ICTs facilities for combating financial crime is shown in Figure 4.2 below

Figure 4.2 Rating the quality of availability of ICTs facilities for combating financial crime



Source: Field Data, 2013

Respondents were asked to rate the qualities of the available ICTs for combating financial crime to determine whether these facilities are high or low in financial crime combating. From the responses received, most (47%) of the respondents rate the available ICTs for combating financial crime as moderate followed by 32% of the respondents who indicated that the available ICTs for combating financial crime were very low, 3% of the respondents indicated high whilst 18% of the respondents also of the opinion that ICTs for financial crime combating were low. As the findings revealed, it can be deduced that ICTs usage in combating financial crime is moderate.

4.4 Types and Level of Financial Crime in GHANA

The second objective of the study sought to determine the types and level of financial crime in Ghana. According to Beeko (2012), there are voluminous financial transactions that are carried out in the cyberspace with no physical boundaries. The cyberspace, a medium which

is oblivious of time and territorial sovereignty, brings instantaneous interconnections all over the world. The methods with which these illegal practices are consummated have become more sophisticated with rapid changes in technology and globalization which Ghana is of no exception. Based on this assertion and the objectives of the study respondents were asked to identify the type of financial crime that commercial unit of the police service deal with. Table 4.6 depicts the type of financial crime in Ghana.

Table 4.6 Type of financial crime outfit deal with most

Type of financial crime	Frequency	Percent
Bank fraud	13	34.2
Debit card fraud	1	2.6
Money laundering	4	10.5
Identity deception fraud	11	28.9
Unauthorised access transfer of money	2	5.3
Hacking into organisational databases	5	13.2
ATM fraud	2	5.3
Total	38	100.0

Source: Field Data, 2013

As shown in Table 4.6 the most financial crime that Commercial Unit of the Ghana Police deals with were bank fraud with 34.2%, Identity deception fraud (28.9%), Hacking into organisational databases (13.2%), Money laundering (10.5%), Unauthorised access transfer of money and ATM fraud with 5.3% respectively. Other financial crimes were Debit card fraud with (2.6%). From the findings, it can be said that Commercial Crime Unit of Ghana Police Service deals with a lot of financial crimes mostly.

Table 4.7 Estimation of institutions suffering from financial crimes in Ghana

Institutions suffering from financial crimes	Frequency	Percent
Banks	16	42.1
Mutual funds	2	5.3
Credit unions	2	5.3
Private businesses	8	21.1
Individuals	10	26.3
Total	38	100.0

Source: Field Data, 2013

Estimation of institutions suffering from financial crimes in Ghana was assessed. During the assessment, it was revealed that banks with responses of (42.1%) were estimated first followed by individuals with (26.3%) responses suffer financial crime in Ghana mostly. Other respondents 21.1% indicated that private businesses also suffers from financial crimes in Ghana mostly whilst mutual funds and credit unions with 5.3% responses respectively were among the institutions that suffers from financial crimes in Ghana mostly.

4.4.1 Bodies most report financial crime to the Commercial Crime Unit (GPS)

As the type of financial crime was known in Table 4.6 and 4.7, the researcher wanted to know which body (institutions) mostly report financial crime to the outfit. The findings from Table 4.8 below show that majority of the institutions that report to the Commercial Crime Unit of Ghana Police Service concerning financial crime were individuals with (50%) responses out of the total sampled for the study followed by the banks with (23.7%) responses.

Table 4.8 Bodies mostly report financial crime to CCU of GPS

Report financial crime	Frequency	Percent
Banks	9	23.7
Credit unions	2	5.3
Private businesses	8	21.1
Individuals	19	50.0
Total	38	100.0

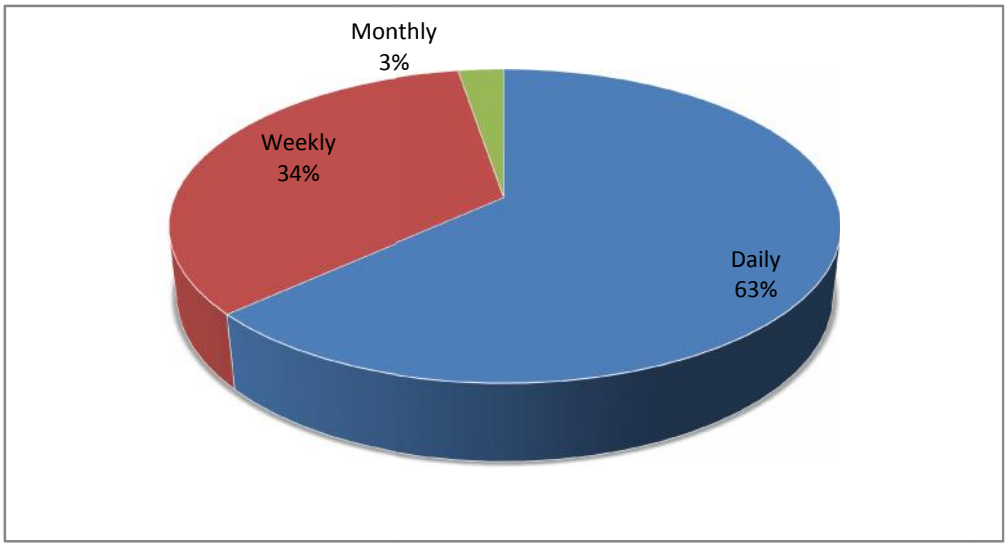
Source: Field Data, 2013

Other bodies that report to the CCU of GPS were private businesses with 21.1% and credit unions with 5.3% of the total responses. It can be concluded that individuals, banks and private businesses were most bodies that report to the CCU of GPS. The implication of this is that these institutions suffer ICTs- based financial crime.

4.4.2 Receiving report of financial crimes

As follow up question, the researcher wanted to know how often do the CCU of GPS received reports on financial crimes in the unit was posed to determine how regularly these crimes are reported. To this, 24 out of 38 representing 63.2% of the respondents indicated that they receive financial reports on daily basis, 13 representing 34.2% of the respondents also indicated that they received financial reports weekly whilst 1 representing 2.6% of the total population sampled indicated that the outfit received reports monthly. As depicted in the Figure 4.3, it can be concluded that financial crime are reported to the CCU outfit on daily basis or weekly.

Figure 4.3 Reports of financial crimes



Source: Field Data, 2013

When respondents were asked to estimated average number of financial crime reports to the CCU outfit, it was estimated that for daily they received a report of financial crime ranging from 1-20. For weekly, it was estimated at 21-40, monthly was estimated at 41-120, and quarterly was estimated at 121-360 reports, whilst half yearly was estimated at 361-674 and yearly was estimated at 675-1350 reports averagely received by the outfit.

Table 4. 9 Estimated average number of financial reports

Frequency	**Number of reported financial crimes**
Daily	1-20
Weekly	21-40
Monthly	41-120
Quarterly	121-360
Half yearly	361-674
Yearly	675-1350

Source: Field Data, 2013

From the analysis it can be concluded that there are a number of reported case of financial crimes.

4.5 Competency for Financial Crime Combat

The third objective of this study sought to find out how competences are the personnel for financial crime combat. In finding out, four questions were posed t the respondents to answer. The first question was what is your outfits' commonest means of detecting financial crimes? Answers to this question were depicted in the Table 4.10

Table 4.10 Commonest means of detecting financial crimes

Commonest means of detecting financial crimes	Frequency	Percent
Multiple-instruction detection system	18	60.5
Routers for incoming traffic from other network	7	18.4
Others specify (statement of a/c and transaction slips of ATMs and withdrawer forms).	8	21.1
Total	38	100.0

Source: Field Data, 2013

The outfit commonest means of detecting financial crimes were through multiple-instruction detection system and routers for incoming traffic from other network. Other means of detecting financial crime are through the use bank statement of account, and transaction slips of ATMs and identifying the account holder or withdrawer forms to trace the culprit as shown in Table 4.10.

4.5.1 Approaches in dealing with financial crimes

When respondents were asked which of the following best described their approaches in dealing with financial crimes, most (42.1%) of the respondents indicated that they use passive response to act on the complaints that are lodged with the unit and act after.

Table 4.11 Approaches in dealing with financial crimes

Dealing with financial crimes	Frequency	Percent
Automatic system alert	9	23.7
Preventive approach (actively involved in dealing with it)	13	34.2
Passive response (response only to complaints and act after	16	42.1
Total	38	100.0

Source: Field Data, 2013

Other respondents 34.2% also indicated that their best approach in dealing with financial crime is preventive approach (actively involved in dealing with it) whilst 23.7% of the respondents also indicated that their best approach in dealing with financial crimes is through automatic system alert. Respondents further explained that this automatic alert system helps them to arrest the culprit on the spot.

Table 4.12 Level of skills in using the ICT facilities in combating financial crime

Level of skills in using the ICT facilities	Frequency	Percent
Very low	10	26.3
Low	8	21.1
Moderate	13	34.2
High	7	18.4
Total	38	100.0

Source: Field Data, 2013

Level of skills in using the ICT facilities was sought to determine whether personnel are highly skills in using ICT in combating financial crime or low in skills. From the data gathered, it was revealed that most (34.2%) of the respondents were moderate in skills of use of ICT, 26.3% of the respondents indicated that their skills in using ICT facilities in combating financial crime very low followed by 21.1% who are low as against 18.4% who

are high in skills for using ICT in combating financial crime. From all indication, it can be concluded that majority of the personnel have a very low skills in using ICT in combating financial crimes.

Table 4.13 Training in the use in the use of ICTs for combating financial crime

Training	Frequency	Percent
Once every 3 months	1	2.6
Twice a year	4	10.5
Yearly	13	34.2
Never	17	44.7
Once a while	3	7.9
Total	38	100.0

Source: Field Data, 2013

As a follow up question, the researcher wanted to know how often personnel of the Commercial Crime Unit receive training in the use of ICTs for combating financial crime. Table 4.13 above shows that most of the personnel 17 (44.7%) never receive any training in the use of ICTs for combating financial crime. Although majority never receive any training, 13 (34.2%) of the respondents indicated that they received training in the use of ICTs for combating financial crime yearly, 4 (10.5%) said they received training in the use of ICTs for financial crime combating twice a year, 3(7.9%) said they do received training once a while followed by 2.6% of the respondents who indicated that they receive training once every 3 months. From the data analysis one can said that ICT training do not have much importance in the police service.

4.6 Challenges in Using the ICT for Combating Financial Crime

The last objective of the study was to find out the challenges in using ICT to combat financial crime. To this, several challenges were raised. The important once among them were: the personnel were not trained on how to use ICT to combat financial crimes, lack of genuine detection softwares, lack of computer forensic experts and forensic systems, investigators have little knowledge of ICT usage, inadequate logistics and other information systems that can be used in combating financial crimes, lack of computers to work with, inadequate modern ICT facilities, lack of network facilities, lack of cooperation on the part of the complainants, lack of assistance from banking institutions to furnish the police with necessary information, and lack of ICT facilities and training experts.

A cursory look at the problems enumerated by the respondents' means that the commercial crime unit of Ghana Police Service do not have the necessary prerequisites in combating ICT-based financial crime.

Table 4.14 How challenges have affected the outfit of CCU/GPS

Challenges	Frequency	Percent
Not at all in any way	1	2.6
To some extent	9	23.7
To a large extent	16	42.1
To a very large extent	12	31.6
Total	38	86.8

Source: Field Data, 2013

In order to determine how ICT challenges have affected the outfit of the CCU/GPS in an attempt to combat financial crime, question was posed to that effect. The responses in Table 4.14 showed that 16 (42.1%) of the respondents indicated that it has affected the outfit to a large extent, 12 (31.6%) respondents also indicated that it has affected the outfit to a very

large extent, 9 (23.7%) of the respondents also indicated that it has affected the outfit to some extent whilst one out of 38 representing 2.6% indicated that it does not at all in any way affected the outfit of commercial crime unit of Ghana Police Service. With majority carries the vote, it can be concluded that ICT challenges has affected the outfit in several ways in combating financial crime.

4.6.1 Suggestions for improvement of the use of ICT in combating financial crimes

Opinions were sought from the respondents on how to improve the level of usage of ICT in combating financial crimes service. Some of the opinions espoused by the respondents were that, the personnel need to be trained in the use of ICT-based financial crimes. Other respondents are expressed that there is the need for the service as whole to train all the service personnel on how to use ICT in combating crimes not necessarily financial crime but all the crimes that got to do with ICT based. Another suggestion were that the commercial crime unit of the police service need to be well resourced with modern ICT facilities, more computers with genuine softwares and corporations between the institutions, individuals and private businesses to combat financial crime.

4.7 Discussion of Findings

From the study it was revealed that availability and adequacy of ICT facilities for financial crime combating was low. To this finding, Harris (2007) argued that there are several commentators who have argued that we are in the beginning stages of a second technological revolution, which will once again dramatically change police organization and administration (Harris, 2007). In support to Harris's (2007) assertion, Hummer (2007) has stated the acquisition of a wide range of additional hardware technology innovations support the design,

development, implementation, and impact of crime prevention and police technology innovations.

4.7.1 Type and level of financial crime in Ghana

The research gathered that the following financial crimes are prevalent in Ghana. These include bank fraud, ATM fraud, identity deception fraud and hacking into organisations' databases. According to Muhammed–Nasiru and Kasimu (2012), information and communication technologies (ICTs) are serving as tools for information gathering and financial crime prevention and detection which remain a vital aspect of combating financial crime. It is important to note that security management has become an issue of all. The contribution of ICT in security management goes beyond the comprehension of the ordinary man on the street. However, at this critical stage of information age, where insecurity of financial institutions, individuals and private businesses remain as issue of worry, the employment of (ICTs) seems vital.

4.7.2 Competency for financial crime combat

With regard to competency for financial crime combat, the study revealed that the commonest means of detecting these financial crimes is through multiple instruction system. For the commercial crime unit to successfully combat this cancer there is the need for special training for personnel. In line with this, Byrne and Gary (2011) are of the view that in crime prevention, there is the need for special control mechanisms (e.g. the deterrent effects of police, courts, and corrections) and informal social control mechanisms, with a focus on the influence (through mechanisms such as attachment, commitment, and involvement) of personnel. In addition, crime prevention strategies have been targeted on different levels of prevention (primary, secondary, tertiary) and on the need for individual (i.e. private actions),

parochial (group actions by neighbourhood residents), and public actions (i.e. decisions to call the police) to prevent crime (Byrne and Gary, 2011). Similarly, Broadhurst (2005) notes that, the effective control of financial crime requires more than cooperation between public and private security agencies. He argued that the role of the communications and IT industries must join hand with the police service to combat financial crime.

4.7.3 Challenges of ICT in combating financial crime

The study also shows that the challenges in using the ICT to combat financial crime effectively are due to lack of adequate training of personnel to build their capacity in this direction. Again, the analysis revealed that commercial crime unit of Ghana Police Service is woefully under resourced with ICT facilities to combat ICT-based financial crime. Byrne and Gary (2011) contended that new technological innovations have been developed to prevent crime and to improve the performance of the police, but the study shows that neither the personnel are well trained nor the nor ICT facilities available.

Harris and Lurigio (2007) point out that one of the major paradoxes related to the development and expansion of risk-assessment technology in the area of violence prevention is that practitioners seem obsessed by the need to assess risk in groups of individuals (e.g. sex offenders) with very low failure rates. For some offender groups, risk appears much less important than stakes; for sex offenders in particular, it appears that the possibility of re-offending is more important than the probability of re-offending (Byrne, 2009).

In addition, Harris and Lurigio (2007) examined the development of new threat assessment protocols, and observe the following: threat assessment involves instruments or protocols to prevent ICT-based financial crime. However, from the study there is no such system in place

as result the personnel are mostly engaged in passive response (response only to complains and act after the crime).

The researcher concludes from the available research that financial institutions, individuals, private businesses are prone to ICT-based financial crime unless the challenges identified are well addressed.

REFERENCES

Beeko, W. (2012). *Fighting Economic and Financial Crimes under the Rule of Law*: *Research Findings*. Retrieved 20/Sept/2013 from www.ghanaweb.com

Byrne, J. and Gary, M. (2011). Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact. *Cahiers Polities studies Jaargang*, vol. 3, No. 20**,** pp. 17-40.

Harris, A. and Lurigio, A. (2007). Crime Prevention and Soft Technology: Risk Assessment, Threat Assessment, and the Prevention of Violence in Byrne, J. and Rebovich, D. (2007). *The New technology of Crime, Law and Social Control* (Monsey, NY: Criminal Justice Press), p 103-132.

Susan, M., Gakure1, R.W., Kiraithe, E.K. and Waititu1, A.G. (2013). The Influence of Resource Availability and Utilization on the Performance of the Police Force: A case study of Nairobi Police Force. *Journal of Business Management and Corporate Affairs*, Vol.2, Issue 1, pp. 1-10.

CHAPTER FIVE

SUMMARY OF FINDINGS, CONCLUSION AND RECOMMENDATIONS

5.1. Introduction

In this chapter, the researcher provides the summary of the key findings and draws conclusions to the study and also makes recommendations based on the findings of the study. The objectives of the study were to:

1. assess the ICT facilities currently in use for combating financial crime in Ghana by GPS
2. to determine the level of use of the available ICT's for combating financial crime
3. to ascertain the competency level of the GPS in using ICT for combating financial crime in Ghana
4. determine the type and level of financial crime activities in Ghana.

Thus, the purpose of the study was to examine the use of information communication technology (ICT) to combat financial crime in Ghana and to identify possible problems and to make recommendations for the proper usage of ICT in the Police Service. The case study was the Commercial Crime Unit of the Ghana Police Service, Headquarters. To guide the research, the adaptive information security systems model was adopted as a theoretical framework for the study.

5.2. Summary of Findings

The summary of the findings have been presented according to the themes in the questionnaire which covered the objectives of the study.

5.2.1 Age

The findings with regard to age and use of ICT facilities revealed that all the personnel especially commercial crime unit of Ghana Police service use ICT resources in one form or other indicating that using ICT facilities did not necessarily depend on age but rather the skill and technical knowhow.

5.2.2 Level of Education

The findings revealed that majority of the personnel had higher levels of education. The higher level of educational attainment by majority of the respondents meant that, they could easily use and fully exploit the necessary ICT facilities for effective combating of financial crime in the country.

5.2.3 Availability and adequacy of ICT facilities for combating financial crime

The study established that the Ghana Police Service have few ICT facilities which are being used in their operations for financial crime combating but lack modern ICT facilities that need to aid them for efficient detection of crime at any time. The study also revealed that ICT facilities for financial crime combating were very low.

5.2.4 Type and level of financial crime in Ghana

From the findings, it was revealed that the type and level of financial crime that the Ghana Police Service deals with were bank fraud, individuals victims of internet fraud, private businesses Internet fraud and identity deception fraud and these has made these body institution mostly suffers from financial crime. The study also show that these financial crimes are reported to the CCU outfit by the banks, private businesses and individuals reported on daily and weekly basis accumulated to monthly, and monthly accumulation to quarterly, half yearly and finally accumulation to yearly report.

5.2.5 Competency for financial crime combat

The study established that the commonest means of detecting financial crimes by the Commercial Crime Unit of Ghana Police Service was multiple-instruction detection system and using statement of account and transaction slips of ATMs and withdrawer forms to detect the financial crime.

Also evident from the study was that most of the personnel skills in of use of ICT was skills in ICT usage was moderate as 34.2% as against 26.3% of the personnel who also indicated that their skills in using ICT facilities in combating financial crime very low.

5.2.5.1 Training in the use of ICTs for combating financial crime

The study found out that majority of the personnel do not receive training on ICT and this need to be carried out regularly to trained the personnel.

5.2.6 Challenges in using the ICT for combating financial crime

The study found that the Commercial Crime Unit of Ghana Police Service faced a lot of challenges in attempts to combat ICT-based financial crime. Some of the major challenges were lack of ICT trained personnel on how to use ICT to combat financial crimes, lack of genuine detection softwares, inadequate logistics, lack of computers, lack of network facilities and lack of ICT facilities and training experts. The findings also indicated that these challenges have affected the outfit of the Ghana Police Service to a large extent.

Evidence from the study indicated that there was the need for prompt and effective training of the Ghana Police Service especially Commercial Crime Unit as the findings revealed that majority of the personnel have low skills in the use of ICT-based in combating financial crime and this was identified as a serious constraint to ICT adoption.

There was the need for every personnel of GPS to have some form of training on how to computers or personnel be trained in order to acquire necessary skills for accessing and utilise ICT facilities and resources. The adoption of ICT facilities and resources would, as a result, improved financial crime detection. It can be concluded from the findings of the study that the when Police personnel are trained in the use of ICT in their service delivery can help combat financial crime in the country.

5.3 Conclusion

This study concludes that ICT-based financial crime is an inevitable downside of the convergence of ICT and that organization and individuals consequently have a duty of ensuring their own protection. The researcher agreed that ICT-based financial crime is common in both developed and developing countries, its impact appears to be worse in developing countries where the technology and laws enforcement expertise is inadequate. Undeniably, the ICT offers significant benefit to the Ghana Police Service if modern ICT facilities are provided and personnel are trained will help in combating financial crime in the country and for the economic, technological, and cultural dividends. Despite major barriers faced by GPS/CCU as a result of low literacy rates and lack of appropriate infrastructure, the ICT facilities remain a source of unlimited opportunities.

Finally, it should be noted that financial crime poses one of the biggest threats to the wide spread development and utilization of ICT around the globe. Whether in the form of hacking, economic espionage, web defacement, sabotage of data, viruses, fraud, unauthorized access to or disclosure of data, or other acts against computers, networks, and data, cyber crime affects everyone – businesses, government, and citizens. Thus, the tasks of identifying ICT-based financial crime as a tool for bringing them to justice pose formidable challenges to law enforcement agencies precisely Commercial Crime Unit of the Ghana Police Service.

5.4 Recommendations

Based on the findings of the study, the following recommendations were made for improvement of ICT facilities for combating financial crime, type and level of financial crime in Ghana, competency for financial crime combat, challenges in using the ICT for combating financial crime to enhance information provision to Ghana Police Service.

5.4.1. ICT Models

It is recommended that appropriate ICT models must be developed to meet the Police information needs considering the ICT-based financial crime and constraints with some field testing within the existing infrastructure. Biometric scanner, PC tracking system, retinal scanner Internet, voice biometrics, intrusion detection system software among others will be suitable in helping the GPS/CCU to deal with ICT-based financial crime. In relation to this recommendation, Broadhurst (2005) attest that, now many public police agencies in ICT advanced nations have recognised the increased interdependence of global markets and have responded to the general risks of cyber crime especially to commerce and financial services. For example, the response of the Hong Kong Police is typical and its mission broadly reflects the scope of public policing now required maintaining a professional investigation capability and broadening the investigation i.e. specialising and mainstreaming expertise; developing accredited computer forensics, proposing changes in laws and policies, prevention and education; intelligence management, and liaison with industry and professionals; and liaison with overseas law enforcement agencies and international MLA cooperation.

Each of these goals needs to be informed by adequately resourced research capable of informing the operational demands of the comprehensive role envisaged by public policing agencies. A highly useful function is formal risk assessment (Grabosky and Broadhurst, 2005). However, how best to promote public education about on-line crime prevention is

equally important. Other issues that require both primary and policy research (often with a comparative context) are for example, the modus operandi of 'new' crimes exploiting new forms of ICT; the most efficient means to train law enforcement agents; the optimum periods to compel ISPs to store traffic or content data; the impact of 'virtual deterrence' in the on-line environment, the characteristics of user responses to security emergencies, patch compliance and other attributes of effective crime prevention; how individuals and private industry can contribute to their own security; and the investigative protocols to apply in the proactive identification of unlawful conduct on the Internet.

5.4.2. Information on ICT facilities

The ICT models must be generated to provide a framework for various stakeholders in Ghana Police Service and also design and implement effective ICT based solutions for all personnel in the ten regions of Ghana to help combat financial crime in the country.

5.4.3. Creation of ICT Awareness

There is the need for ICT awareness creation among the police service to be aware of its usefulness. In order to create awareness level among the police service, ICT experts should be employed to embark on training regularly to equip the personnel to become effective in use of ICT facilities in service delivery.

5.4.4. User training and Education

Adequate user training and education should be given to all Police personnel in the use of ICT facilities. There must be planned and continuous programmes of training for police personnel at all ranks. The rapid developments in ICT make the need for regular training even more essential, and the importance of networking and access to other information sources should be included in training programmes.

5.4.5. Engagement of Information Professionals

As the study has shown the low usage of ICT facilities, respondents indicated that most of them were not trained to use the ICT on their own. They also do not have the knowledge of modern technologies being used by the criminal. Modern ICT facilities need to be provided to them in good time and in precise form to enable them know more about how to use these ICT facilities in combating financial crime and for better output and higher operations.

5.4.6 Increased provision of ICT facilities

The Ghana Police Service should provide the needed ICT facilities to control some of the problems that hinder the effective use of the ICT facilities and services. These measures should include acquiring genuine software, frequent training, and seminars for the personnel on the importance of use of ICT in combating financial crime.

Generally, it is recommended that the availability of broadband in Ghana have to be inculcated into police activities in fighting financial crime. This broadband must help solve some of the challenges GPS face in handling ICT-based in combing financial crime. More ICT facilities should be provided and maintained so all the security agencies in the country can benefit from it.

5.4.7 International/National Associations Collaboration

Also, from the findings there is the need for improve networking, cooperation and collaborations among professionals for example, UN and other security agencies that are well vested in the use of ICT in combating financial crime should call upon to resource the Ghana police service with ICT facilities and training to encourage resource sharing.

BIBLIOGRAPHY

Abor, J. (2004). *Technological Innovations and Banking in Ghana: An Evaluation of Customers' Perceptions. American Academy of Financial Management.* Retrieved from: www.financialanalyst.org, (Accessed on: January 28, 2013).

Aidoo, D. B., Akotoye, F.X.K., & Ayebi-Arthur, K**.** (2012). Academic 419: Locating computer crimes in the use of ICT for the management of educational systems in Ghana – The case of University of Cape Coast. *Journal of Educational Management*, vol. 6, pp.102-111.

Anderson, M.L. and Taylor, H.F. (2009). *Sociology: The Essentials*. Belmont, CA: Thomson Wadsworth.

Beeko, W. (2012). *Fighting Economic and Financial Crimes under the Rule of Law. Research Findings from* www.ghanaweb.com

Bell, J. (2005). *Doing Your Research Project* 4th ed., Buckingham: Open University Press.

BiztechAfrica, (2011). *Ghana to curb cyber crime*. Retrieved November 30, 2013, from http://www.biztechafrica.com/article/ghana-moves-curb-cyber-crime/1533/

Broadhurst, R.G. (2005). *International Cooperation in Cyber-crime Research*. In Proceedings 11th UN Congress on Crime Prevention and Criminal Justice, Workshop 6:'Measures to Combat Computer Related Crime', pages pp. 1-12, Bangkok.

Bryman, A. And Bell, E. (2007). *Business Research Methods* 2nd ed. Oxford: Oxford University Press.

Byrne, J. and Gary, M. (2011). Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact. *Cahiers Polities studies Jaargang*, Vol. 3, No. 20**,** pp. 17-40.

Byrne, J. (2009). *The New Generation of Concentrated Community Supervision Strategies: Focusing Resources on High Risk Offenders, Times, and Places. (Washington, DC: A Report for the Public Safety Performance Project, the Pew Charitable Trusts)*. Retrieved on 01/12/2013 from https://www.ncjrs.gov/pdffiles1/nij/238011.pdf

Bureau of Justice Assistance (2009). *Internet Crime report, Internet Crime complaint centre, Bureau of Justice Assistance, US Department of Justice*, http://www.ic3.gov/media/annualreport/2009 _IC3Report.pdf, 2013.

Citifmonline (2011). *Ghana among top 10 on global internet fraud table*. Availabe at http://www.citifmonline.com/index.php?id=1.287156.1.420460 Jun 10.

Charney, S. and Alexander, K. (2001). *Computer Crime Research Centre*. Retrieved 15, November, 2013 from http://www.crime-research.org/library/Alex.htm

Chawki, M. (2009). *A Critical Look at the Regulation of Cybercrime*. Retrieved on November 30, 2011 from http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2009_1/chawki/chawki.pdf

Creswell, J. (2003). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches* 2nd ed. London: SAGE Publications.

Crossman, A. (2013). *An Overview of quantitative research methods: surveys, secondary data, and experiments*. Retrieved on 02/12/2013 from http://sociology.about.com/od/Research/a/Overview-Of-Quantitative-Research-Methods.htm

Daily Guide (2013). *Fight financial crime through vigilance*. *Business News of Wednesday*, 23 October 2013 Retrieved on 06/12/2013 from http://www.ghanaweb.com/GhanaHomePage/NewsArchive/artikel.php?ID=289684

Dawson, C. (2009). *Introduction to Research Methods: A Practical Guide for Anyone Undertaking a Research Project*. 4th ed., Oxford: How to Books Ltd.

Dugo, H (2008). *Journalists Appropriation of ICTs in News Gathering and Processing*. Rhodes University.

Bosworth, B.P. and Triplett, J.E. (2000). *What's new about the New Economy? It, Economic Growth and Productivity', Brookings Economic Papers*, October 20.

Fraenkel, J. R. and Wallen, N. E. (2000). *How to Design and Evaluate Research in Education* 4th ed., New York: McGraw–Hill, p. 101.

Folarin, S. (2009). The Anti-Corruption War in Nigeria: A Critical Appraisal of the Role of the ICPC and EFCC", Nigerian. *Journal of Economic & Financial Crimes*, Vol. 1 No. 2, pp.14-36

Ghana Business News (2009). *Ghana Business News Cyber crime: Giving a bad name to Ghana February 17*. Retrieved on 20/11/2013from http://www.ghanabusinessnews.com/2009/02/17/cyber-crime-giving-a-bad-name-to-ghana/

Ghana Business News (2012). *Ghana Police Launches E-Crime Project*. Retrieved from: http://www.ghanabusinessnews.com/ghana-police-launches-e-crime-project, (Accessed on: January 30, 2013).

Gharoro, EP, Igbafe, A.A. (2000). Pattern of drug use amongst antenatal patients in Benin City, Nigeria. *Med Sci Monit*, Vol. 6, No.1, pp.84–87.

Grabosky P., and Broadhurst, R.G. (2005). *The Future of Cyber-crime in Asia',* in Broadhurst, R.G & P. Grabosky [Eds.], *Cybercrime: The Challenge in Asia*, The University of Hong Kong Press, pp. 347-360

Greer, C (2010). *Crime and Media***:** A Reader. London: Routledge.

Gee, G. and Kim, P. (2011). *Doppelganger Domains*. Retrieved 15 September from files.godaigroup.net/doppelganger/Doppelganger. Domains.pdf

Gottschalk, P. (2010). *Policing Cyber Crime*. Routledge: Petter Gottschalk and Ventus Publishing ApS.

Harris, A. and Lurigio, A. (2007). Crime Prevention and Soft Technology: Risk Assessment, Threat Assessment, and the Prevention of Violence. In Byrne, J. and Rebovich, D. (2007). *The New technology of Crime, Law and Social Control* (Monsey, NY: Criminal Justice Press), p. 103-132.

Healey, F. J. (1993). *Statistics: A Tool for Social Research* 3rd ed., Belmont: Wadsworth**.**

Hummer, D. (2007). *Policing and "Hard" Technology* In: Byrne, J. and Rebovich, D. (2007). *The New technology of Crime, Law and Social Control,* Monsey, NY: Criminal Justice Press, p. 133-152**.**

Ibezimako, M. (2006). Information and Communication Technologist. (ICTs) in Modern Public Relations Practice: Uses, Impact. In Mass Media Review. *An International Journal of Mass Communication*.

Idogho and Ogedegbe (2010). The Role of ICT in Poverty Reduction in Nigeria. *The Journal of Arts, Management Science and ETF Project*.

Ivancevich, J.M. (2004). *Human Resource Management*. New York: McGraw –Hill.

Jackson, L.S. (2011). *Research Methods: A Modular Approach* 2nd ed. New York: Wadsworth/Cengage Learning.

Kabay, M.E. (2008). *Computer Security Handbook*, 5th ed. New York: Wiley.

Kumar, R. (2005). *Research Methodology: a Step-by-Step Guide to Beginners* 2nd ed., London: SAGE Publications.

Lachlan, K. (2004). *Introduction to Mass Media*. United States of American: Kendall / Hunt Publishing Company.

Leman-Langlois, S. (2008). *Technology, crime and social control*. Manitoba: Willan Publishing.

McQuail, D. (2005). *Communication Theory* 5th ed. London: Sage Publication.

Moin, I.K. and Ahmed, B.Q. (2012). Use of data mining in banking. *Int. J. Eng. Res. Appl*., vol. 2, No.2, pp. 738-742.

Muhammed–Nasiru, I. and Kasimu, S. (2012). *Surveillance, Information and Communication Technologies (ICTS) as tools for information gathering and security management department of mass communication, school of information and communication technology (ICT),* Auchi polytechnic, Auchi.

Mwakalinga, J. and Kowalski, S. (2011). ICT Crime Cases Autopsy: Using the Adaptive Information Security Systems Model to Improve ICT Security. *International Journal of Computer 114 Science and Network Security*, vol.11 No.3, pp.1-10.

Myjoyonline.com (2012). *Police turns to ICT to fight crime*. General News of Saturday, 18 February. Retrieved on 03/12/2013 from http://www.ghanaweb.com/GhanaHomePage/NewsArchive/artikel.php?ID=230212

Negash, S. (2004). Business intelligence. *Commun. Assoc. Inform. Syst*., Vol. 13: pp.177-195.

Neuman, W. L. (2007). *Basics of Social Research: Qualitative and Quantitative Approaches* 2nd ed., New York: Pearson Education Inc.

Nieto, M. (1997). *Public Video Surveillance: Is it an Effective Crime Prevention Tool*?

Nwabueze, C. (2005). *The Art of Investigative Reporting, A Practical Guide*. Enugu: Daisy Press.

Nwosu, I. (2004). Digital Public Relations Concept and Practice. In J. Nkwocha (Ed). Digital Public Relations. Lagos: Zoom len Publishers.

Oak, M. (2009). Intelligent Life on the Web Retrieved 09 September from http://www.buzzle.com/articles/types-of-computer-crimes.html

Obaze, A and Fashanu, F (2006). *Mass Communication Law and Ethics*. Ibadan: Safmos Publishers.

Okpoko, J. (2009). Understanding International Communication. Zaria: University Press Limited.

Pokoo-Aikins, J.B. (2002). The Police in Ghana 1939-1999. Accra: Rescue Printing Press.

Paulsen, D.J. (2009). A Discussion of Technology and those who use it for criminal gain. Retrieved on 28/11/2013 from http://www.criminalbehavior.com/Spring2009/Section%201 %20Hackers.pdf

Petrini, M. and Pozzebon, M. (2003). The value of "business intelligence" in the context of developing countries. Proceedings of 11th European Conference on Information Systems, Napoli, Italy.

Prasad, J.N., Kathawala, Y., Bocker, H.J. & Sprague, D. (2003).The Global Problem of Computer Crimes and the Need for Security. *Industrial Management*, 24-28.

Rao, K.G. and S. Dey (2012). An intelligent decision making architecture for banks: Business intelligence and knowledge management systems integration. *J. Econ. Develop. Manag. IT*, 4(1): 49-63.

Rogers, M. (2001). A new hacker Taxonomy, Department of Psychology University of Manitoba, Winnipeg RSA Security Conference.

Rollins, J., Wyler, S. L. (2010) International Terrorism and Transnational Crime: Security Threats, U.S. Policy, and Considerations for Congress Retrieved December 15, 2011 from http://www.fas.org/sgp/crs/terror/R41004.pdf

Rosen, J (2004). *The Naked crowd*: Reclaiming security and Freedom in an Anxious Age. New York: Random House.

Salwan, D. (2008). *Business intelligence in financial institutions. Proceedings of the 2nd National Conference,* IndiaCom. New Delhi, India: JAY Publishers.

Saunders, K. and Zucker, B. (1999) 'Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act', in Wall, D. (ed), special issue on E-Commerce, *International Review of Law, Computers and Technology*, vol.13, no. 2

Saunders, A. and Cornett, M. (2008). Financial Institutions Management: A Risk Management Approach. 6th Edn., McGraw-Hill, Irwin, New York, pp: 2.

Schneider, F. and Enste, D.H. (2000). *'Shadow Economies: Size, Causes, and Consequences'*. Journal of Economic Literature, Vol. 38, pp.77-114,.

Singh, R.S. (2008).Encyclopaedia of Library Science Today. New Delhi: ANMOL Publications PVT. Ltd.

Sourcingfocus.com, (2012). UNISYS: Using Big Data Analytics to Fight Financial Crime. Retrieved from: http://www.sourcingfocus.com/uploaded/documents/Unisys_Using_big_data_analytics_to_fight_financial_crime.pdf (Accessed on: November 30, 2013).

Susan, M., Gakure1, R.W., Kiraithe, E.K. and Waititu1, A.G. (2013). The Influence of Resource Availability and Utilization on the Performance of the Police Force: A case study of Nairobi Police Force. Journal of Business Management and Corporate Affairs, Vol.2, Issue 1, pp. 1-10.

Surette, R (2007). Media, Crime and Criminal Justice: Images, Realities and Policies, 3rd Edition. Belmont, CA: Thomson Wadsworth.

Tabiri, C. (2012). ICT and the Provision of Agricultural Information for Cashew Farmers in Ghana: A Case Study of Techiman in the Brong Ahafo Region. M PHIL thesis, Department of Information Studies, University of Ghana.

Taylor, D. (2012).The Literature Review: A Few Tips on Conducting It. Retrieved on 17/12/2013 from www.writing.utoronto.ca

Telecoms, Internet and Broadcast in Africa, (2007) Telecoms, Internet and Broadcast in Africa Issue no 349 8th April 2007 POLICE ADVOCATE FOR LAWS TO COMBAT CYBER FRAUD IN GHANA Retrieved 10 October from

http://www.balancingact-africa.com/news/en/issue-no-349/computing/police-advocate-for/en

Turban, E., R. Sharda and D. Delen, (2011). Decision Support Systems and Intelligent Systems 9th ed., New York Prentice Hall International.

Twum, 2011).

United Nations Office on Drugs and Crime (2005). *'Bi-Annual Seizure Report 2004/2'*. UNODC, April 2005. Retrieved on 07/12/2013 from http://www.unodc.org/pdf/WDR_2005/volume_1_web.pdf

UNDP (2001) United Nations Development Programme (UNDP), United Nations Office on Drugs and Crime (UNODC). *Corruption. A crime against*... www.yournocounts.org

van Soomeren, P. (2000). Crime prevention solutions for Europe: Designing Out Crime, Conference on the relationship between the physical environment and crime reduction and prevention, Szczecin – Poland.

Victorian Auditor-General's Report (2012).Obsolescence of Frontline ICT: Police and Schools. Retrieved on 03/12/2013 from http://www.audit.vic.gov.au/publications/20120620-ICT-Obsolescence/20120620-ICT-

Wang, S.Y.K. and Huang, W. (2011). The Evolutional the of types of identity thefts and online frauds in the Era of Internet. Journal of Criminology Retrieved on November 12, 2013 from http://www.internetjournalofcriminology.com/Wang_Huang_The_Evolutional_View_of_the_Types_of_Identity_Thefts_and_Online_Frauds_in_the_Era_of_Internet_IJC_Oct_2011.pd

Zack, R. (2009). Information and Communication Revolution in the 21st Century. Lagos: Prime Target Venture.

Zetter, K. (2010). Sarah Palin E-mail Hacker Sentenced to 1 Year in Custody Retrieved 02, November 2011 from http://www.wired.com/threatlevel/2010/11/palin-hacker-sentenced/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+wired27b+%28Blog+-+27B+Stroke+6+%28Threat+Level%29%2

DEPARTMENT OF INFORMATION STUDIES

UNIVERSITY OF GHANA

QUESTIONNAIRE FOR PERSONNEL OF THE CRIME UNIT

Dear Sir/Mad.

The researcher is a final year student of Department of Information Studies, University of Ghana. As a requirement for the award of the Master of Arts in Information Studies, the researcher is conducting a study on **"The use of information communication technology (ICT) to combat financial crime in Ghana: A case study of the Ghana Police Service Commercial Crime Unit"**. I will be very grateful if you could spend few minutes of your busy time to complete this survey questionnaire. The responses you give will be used for academic purposes only. You are also assured of strict confidentiality.

Thank you.

(David Joachim Quanson)

BIO DATA OF RESPONDENTS

1). Age:

1. Below 25 [ ]
2. 26-30 [ ]
3. 31-35 [ ]
4. 36-45 [ ]
5. 46-55 [ ]
6. above 56 [ ]

2). Sex

i. Male [ ]
ii. Female [ ]

3). Highest Educational Level:

i.'O' Level [ ]
ii. A' Level [ ]
iii. SSSCE [ ]
iv. First degree [ ]
v. Master degree [ ]
vii. PHD [ ]
viii. Other specify…….

4). Rank:

i. Constable II [ ]
ii. Lance Corporal [ ]
iii. Corporal [ ]
iv. Sergeant [ ]

v. Inspector [ ]
vi. Chief Inspector [ ]
vii. ASP [ ]
viii. DSP [ ]
ix. SUPT [ ]
x. C/SUPT [ ]
xi. ACP [ ]
xii. DCOP [ ]
xiii. COP [ ]

5). Number of years in the Service? ……

AVAILABILITY AND ADEQUACY OF ICT FACILITIES FOR COMBATING FINANCIAL CRIME

6) What are the ICT facilities available for the GPS?

ICT facilities	Available		Status		Usage	
	Yes	No	Working	Not working	Being used	Not being used
Mobile networks software						
Mobile communication devices						
Biometric scanner						
PC tracking system						
Retinal scanner						
Fingerprint scanner						
Voice biometrics						
Automated Fingerprint Identification System						
Walkie-talkies						
Intrusion detection system software						
Video cameras						
Forensic acoustics						
Other (state)						

7). Indicate the level of adequacy of the following ICT facilities for combating financial crimes

	Very low	Low	Moderate	High	Very High
ICT facilities					
Software					
Hardware					
Personnel					
Skills support					

8). How will you rate the quality of the available ICTs for combating financial crime?
i Very low [ ]

ii Low [ ]
iii Moderate [ ]
iv. High [ ]
v. Very High [ ]

TYPE AND LEVEL OF FINANCIAL CRIME IN GHANA

9). What type of financial crime does you outfit deals with most? (Choose only ONE)
i) Bank fraud [ ]
ii) Debit card fraud [ ]
iii) Money laundering [ ]
iv) Identity deception fraud [ ]
v) Unauthorised access transfer of money [ ]
vi) Hacking into organization databases [ ]
vii) ATM fraud [ ]
viii) Other (state) ……

10). In your estimation, which body or institution most suffers from financial crimes in Ghana?
i. Banks [ ]
ii. Insurance companies [ ]
iii. Mutual funds [ ]
iv. Credit unions [ ]
v. Schools [ ]
vi. Public institutions [ ]
vii. Private businesses [ ]
viii Individuals [ ]
ix. Other specify……..

11). Which body most report financial crimes to your outfit?
i. Banks [ ]
ii. Insurance companies [ ]
iii. Mutual funds [ ]
iv. Credit unions [ ]
v. Schools [ ]
vi. Public institutions [ ]
vii. Private businesses [ ]
viii Individuals [ ]
ix. Other specify……..
12). How often do you receive report of financial crimes in your outfit?
i. Daily [ ]
ii. Weekly [ ]
iii. Monthly [ ]
iv. Quarterly [ ]
v. Half yearly [ ]
vi. Yearly [ ]

13). Please indicate the estimated average numbers of financial crime reports to your outfit:

Frequency	**Number of reported financial crime**

Daily	
Weekly	
Monthly	
Quarterly	
Half yearly	
Yearly	

COMPETENCY FOR FINANCIAL CRIME COMBAT

14). What is your outfits commonest means of detecting these financial crimes?
i. Multiple-instruction detection system [ ]
ii. Routers for incoming traffic from other networks [ ]
ii. Others specify……..

15). Which of the following best describe your approach to dealing with financial crime?
i) Automatic system alert [ ]
ii) Preventive approach (actively involved in dealing with it) [ ]
iii) Passive response (response only to complaints and act after the crime) [ ]

16). What is your level of skills in using the ICT facilities available for financial crime combat?
i Very low [ ]
ii Low [ ]
Moderate [ ]
iv. High [ ]
v. Very High [ ]

17). How often do you receive training in the use of ICTs for combating financial crime?
i. Once every 3months [ ]
ii. Twice a year [ ]
iii. Thrice a year [ ]
iv. Yearly [ ]
vi) Never [ ]
vii. Other (state)……..

Challenges in Using the ICT for Combating Financial Crime

18). What are some of the challenges your outfit faces in its attempts to combat ICT-based financial crimes?
…….
…….
……
……
…….

19). To what extent has these challenges affected your outfits attempts to combat financial crime?
i. Not at all in any way [ ]
ii. Not to a large extent [ ]
iii. To some extent [ ]

iv. To a large extent [ ]
v. To a very large extent [ ]

20). What do you think can be done to improve the level of use of ICT in combating financial crimes……..……
……
……
……
……..

Thank you for your time.

Comments/suggestions: ?????

email address & Contact :0244-502195/0264476513