A SURVEY OF INSIDER INFORMATION SECURITY THREATS MANAGEMENT IN COMMERCIAL BANKS IN KENYA

DOMINIC K.MULWA

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF MASTER OF BUSINESS ADMINISTRATION, SCHOOL OF BUSINESS, UNIVERSITY OF NAIROBI

OCTOBER, 2012

DECLARATION

This research project is my original work and has not been presented for a degree in any other University.

Signed: _____ Date: _____

MULWA D.K.

D61/63021/2010

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

Signed: _____ Date: _____

JOEL K. LELEI

Lecturer

Department of Management Science

University of Nairobi.

DEDICATION

I dedicate this project to my entire family and my supervisor for their hard work, support and encouragement through the entire project.

ACKNOWLEDGEMENTS

This project would not have been possible without the support of people, to whom I recognize below for their contribution.

I would like to express my warm and sincere gratitude to my supervisor, Joel K. Lelei for his continuous guidance and support. His knowledge and advice of research projects was of great help to me. His suggested approaches gave me direction and facilitated in completion of the project. I am extremely grateful and fortunate to have benefit from his brilliance. I would like to thank him for reading my numerous revisions and tirelessly ensured we followed the university guidelines.

I would as well thank all the respondents who took time to fill the questionnaires. It's through their efforts that produced the data used in my analysis.

I would like to thank my family, parents and friends for believing in my interests to pursue MBA and supporting me.

I thank God for the strong courage and determination which has seen me through the course.

TABLE OF CONTENTS

LIST OF TABLES

ABSTRACT

The technological advances in information security have done a lot to contain and even prevent most of the remote or physical threats to information security. However, organizations now face a more subtle and greater information security threat; the insider. This research study is inspired by the emerging question of whether organizations have become more secure or more vulnerable by looking at the insider threat issue. Fraud, much of which includes insider attacks, has tripled in the last 3 years and continues to be a big concern for the banking industry in Kenya. This study seeks to fill the gaps in knowledge and approaches relating to Insider Information Security threats by analyzing the types of information security threats facing commercial banks in Kenya and the mitigation strategies to insider information security threats.

The study made use of the survey research design model. Surveys are more flexible in the sense that a wider range of information is collected. Questionnaires were used to gather data from representatives of the various commercial banks. Statistical methods such as mean, standard deviation and factor analysis were utilized to analyze the data collected from the respondents.

The findings indicate that since most of these mitigation strategies are utilized in many of the banks in various degrees, there is need for them to be fortified with proper training, awareness, motivation, and management of work place issues like workload pressures. While financial gain seems to be an obvious motivation for insiders, other motivations also drive these acts as the study reveals. Frustrated employees for instance may think of harming the organization as a result of their frustration. A key challenge for the banks is the associated cost of information security tools and mitigation strategies. However, the relatively high premium on information security as seen in the increasing reports of the number and magnitude of breaches has compelled organizations to put the matter for consideration in the highest management levels.

Demographic details also points out the age bracket which is prune to the insider threat activities. Banks need to be on the lookout for the below 40 years of age. New recruitments for such staff would require thorough prescreening and as well refresh training on the essence of personal integrity.

The insider threat challenges should be approached comprehensively and must also be viewed as a people problem, rather than the conventional technical approach. Owing to the disconcerting fact that the conventional technical approaches and mitigations will not in themselves secure the modern day organization, there is need for a deeper understanding of insider threats. This study is aimed at providing insights into the insider threats by looking at the banking industry, one of the most important and fastest growing industries in Kenya.

CHAPTER ONE

INTRODUCTION

1.1 Background

Information is an asset which, like other importantbusiness assets, has value to an organization. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever form information takes, or means by which it is shared or stored, it should always be appropriately protected(ISO 17799, 2000).

With the current dynamic technological advances, electronic information has grown in importance. Companies now performing most of their everyday business activities electronically and this has drastically changed level of information security threats. Trustworthy employees who have legitimate access to the information, deliberately or accidentally affect company's business operations. According to Research Foundation (2006), the nature of computer crime has changed over the years as the technology has changed and this has paved the way for criminal activities. Although thrill-seeking hackers are still common, the field is increasingly dominated by professionals who steal information for sale and disgruntled employees who damage systems or steal information for revenge or profit.

External threats to information security have arguably received a lot of publicity due to their frequency, complexity or magnitude. These include physical security breaches, network hacking attempts, viruses and spyware attacks, system sabotage, among others (Schultz, 2002). However, according to researchers and information security experts, attacks from the inside of the organization are now considered more risky and now present a bigger threat because insiders have the access and therefore the wherewithal to

pounce on any vulnerabilities (Baker et al., 2008). They include sabotage, theft and installation of malicious and unauthorized software, social engineering, and viruses.

The insider information securitythreats whichare the basis of fraud and all other nefarious activities are not new. As far back as the 1980's, the insider threat was real and already a headache for many organizations (United Press International, 1981). According to surveys and research reports, the current or the former employees present the greatest information security threat. Further, the frequency and number of these insider threats have increased exponentially in recent years (Greitzer et al., 2008). More concerted efforts are therefore required to prevent the insider threats from growing to unmanageable proportions which could lead to widespread economic losses among others for the modern day organizations.

Industry analysts now infer that fraud and cyber-crime are the most apprehensive issues facing banks today. Insider attacks is now the banking industry's most pressing problem and reports indicating the severity, frequency, and complexity of these concerns are not uncommon. Bankers now grapple with the pessimistic conclusions and facts indicating that the challenge to curb fraud and cyber-crime may be an elusive one. Reputational risks and economic losses are the greatest effects of insider attacks (Ravich, 2011).

1.1.1Insider Information Security Threats

Modern descriptions of Insider will require modern day organizations to expand their risk and threat assessment and analysis to include all parties. According to Brancik (2008), an insider is basically anyone who has the same or similar access rights to an organization, a network system, or an application. This may be a current or former employee, a contractor, a service provider, software vendor, a consultant, or any service provider. An insider threat or attack is therefore considered to be a deliberate misuse and breach on data security by those who are authorized. However, many of these insider threats or

attacks are increasingly becoming the result of complicity between an insider and an outsider.

Tugular and Spafford (1997) have defined malicious insiders as individuals who are capable of using a computing system at an assigned privilege level, but who use the system in a way that bypasses or exceeds this level, thereby violating their organization's information security policy. There are four groups of insiders according to Cole (2010), they include: pure Insider, Insider associate, Insider affiliate, and outside affiliate.

Aeran (2006) offers an overview of the types of threats and attacks that an organization faces through Insider attacks: They include sabotage, theft, viruses, social engineering, online adult activities and installation of unauthorized software. Schmidt (2011) implores a fundamental review of data security. There certainly have been great advances in the technical countermeasures in the last 10 years that are now available but it is still unclear whether we are less vulnerable to fraud and data security breaches. He also implies that the whole concept of 'security' may be a nebulous one; given the recent high profile fraud and security breaches. Further, the banking sector has generally been compelled in recent times to adapt to the unremitting business requirements, largely due to the high rate of advancements in information systems. These have however also opened up the avenues of data exchange and further exacerbated the complexities caused by sharing of data through the various channels, making it more difficult to protect data (Killmeyer, 2006).

Detection of insider attacks is often a difficult and elusive task until the potential damage or loss is obvious as Schultz (2002) notes. This is partly because of the traditional reactive approaches. However, several predictive models of insider characteristics and behavior, most of which are empirically-deduced, have been proposed and are usually easily overlooked, partly because of their subtle nature. They include personality traits (introversion, depression and weaknesses in handling stress/conflict), verbal behavior,

across system usage patterns (unusual usage patterns), negative work environments, preparatory behavior (reconnaissance activity), meaningful errors (errors that indicate malicious intent) and deliberate markers left behind by the attackers.

In mitigating the insider security threats, approaches which are of technical and non-technical have been used. Carroll (2006) states that regulatory compliance is forcing organizations to reconsider how risk management is approached; internal policy is the base for regulatory compliance and insider incident prevention. Policy defines and governs actions and behaviors of personnel within an organization. However, policy by itself is not very useful if it not backed by consequences. These consequences have the greatest impact to the insider threat.

1.1.2Commercial Banks in Kenya

Commercial banks basically act as financial intermediaries that accept deposits and channel those deposits into lending activities. They provide a safe place to keep excess cash and primarily make money by charging higher interest rates on their loans than they pay for the deposits. The changes that new technologies have brought to banking sector are enormous in their impact on employees and customers. Advances in technology are allowing for delivery of banking products and services more conveniently and effectively than ever before - thus creating new bases of competition. Rapid access to critical information and the ability to act quickly and effectively will distinguish the successful banks of the future. The bank gains a vital competitive advantage by having a direct marketing and accountable customer service environment and new, streamlined business processes. Consistent management and decision support systems provide the bank that competitive edge to forge ahead in the banking marketplace.Banks are aware of customer's need for new services and plan to make them available. Information Technology has increased the level of competition and forced them to integrate the new technologies in order to satisfy their customers.The effect on banks is particularly

multifaceted and has inevitably presented a host of opportunities as well as threats and security concerns (Kantankji, 2008).

There are currently 43 commercial banks operating in the country according to the Kenya Bankers Association (KBA, 2012). This body has overseen and steered growth in the industry in its 50-year existence. Some of the milestones have included raising the bar and setting the pace in innovation and technology use in operations. Banks have been at the forefront in innovation and successful implementation of new technology in Kenya according to the association. Specific examples include modernization of the payment systems, the Automated Clearing House, the Credit Reference Bureau, the Real Time Gross Settlement Scheme, Cheque Truncation System, Currency Center Project, and recently even sharing of their Automated Teller Machine (ATM) networks (KBA, 2012).

These advances have however increased the levels of vulnerabilities within the banks and increased the avenues for exploitation considering the increasing threats and effects of insider attacks. Approximately 50 cases of fraud and insider attacks in the financial industry are reported every month according to the Kenya Police 2010 official crime statistics. In December 2010 alone, Ksh. 500 Million was reported from 20 banks and 13 other financial institutions (Mukinda, 2011). It is now imperative for the banking industry to re-imagine information security as the insider threats increase in magnitude and complexity.

1.2Statement of the Problem

According to a global economic survey (GECS, 2011) carried out in 78 countries to provide a global picture of economic crime, revealed that cases of information security breaches are on the rise. There are more opportunities to commit fraud and more pressure to do so. Kenya is on the list of countries that have reported the highest level of fraud in 2011, with a nearly 10% increase from 2009.Information security breaches in the Banking sector continue to be a big concern. According to Kioko (2011), fraud in the

Kenyan banking sector has particularly tripled in 2010 as compared to 2009 and a massive Ksh 3 billion was lost through fraud. Information security breaches and fraud are increasingly proving to be lucrative opportunities as they now cost the global corporate sector an estimated $388 billion annually. While the larger portion of this cost goes towards the security infrastructures that mitigate the threats, an estimated over 30% is direct cash lost through the information breaches and fraud (Standard Digital, 2012).

This study seeks to bring to the fore the need for a review of the insider threat to an organization. The insider threat has for far too long been overlooked by many organizations when conducting their risk and threat analysis assessments. For the organizations that bear the brunt of the insiders' nefarious activities, reputational and financial risks are quite high. The cost of ignoring preventative solutions in the long run is comparatively much higher (Brancik, 2008).Insider threats and risks require assessment, prioritization and, most of all, action rather than reaction. Cole (2008) crystallizes the issue: The insider threat is like a tumor. If you realize there is a problem and address it, you will have short-term suffering but a good chance of recovery. If you ignore it, it will keep getting worse and while you might have short-term enjoyment, it will most likely kill you.

While it may be often difficult and even impossible, organizations should ideally be able to predict and circumvent insider attacks, much like the way clandestine government agencies are able to sniff out and thwart the actions of potential spies through profiling them as Schultz (2002) observes. Like many other crimes, fraud which is perpetrated mainly by insider involvement can be aptly explained by three major factors; a supply of motivated offenders, the availability of suitable targets, and the absence of capable guardians and control systems. A combination of these three major factors lays the ground for all insider attacks (Cohen and Felson, 1979).

Despite the prevalence of the insider threat problem in the modern day organization, there is little systematic study of vulnerable insiders and majority of resources are still being channeled to the development of technologies to detect and prevent external threats. However, the insider threat is essentially a human problem, and human problems cannot be solved with technological solutions. Therefore, insider risk must be assessed and managed if the organization is to make any headway in mitigating its vulnerability to fraud, espionage, or sabotage by those who know the system too well: insiders (Shaw, Ruby and Post, 2005).

This study seeks to fill the gaps in studies, concerns and approaches relating to Insider Information Security threats and seeks answers to the following two research questions: What are the types of information security threats facing commercial banks in Kenya? What are the mitigation strategies to insider information security threats?

1.3Objectives of the Study

The objectives of this study are:

i. To determine the nature of insider threats facing commercial banks in Kenya.
ii. To determine mitigation strategies which commercial banks in Kenya could use to manage insider information security threats.

1.4Value of the Study

Identification, Authentication and Authorization are crucial aspects of the overall security framework and they should be enhanced and become more stringent. However, a technology-centric approach to dealing with the Insider is too narrow in itself and therefore, not equal to the enormous challenge of curbing the issue. This study shall provide a paradigm shift in this respect to the banks, financial institutions, Information and Communication Technology service providers and policy and regulations providers like the government seeking to get a grip on the insider challenge. The findings and

conclusions will be a catalyst and valuable reference as they re-imagine their efforts in dealing with fraud and insider attacks. The results of the study will show that detecting insider threats as early as possible or preventing them altogether requires understanding the psychological, organizational, technical aspects of the problem, and as well as how to coordinate their actions over time. Expected outputs of the study will be the characteristics to be observed on staff with access to computer systems, behavior trends to be monitored, personal and cultural vulnerabilities, the indispensable role of the insider, social and personal frustrations, insider espionage, lack of empathy and reduced loyalty.

The study will elaborate the importance of the Methods of prevention or minimizing the insider security problems by considering Pre-employment screening, Improved Management of Data, Innovative approaches to managing the risks, Comprehensive information security Audits, Enforcement of stringent laws and prohibitive punishments and Training and awareness.Organizations will have insight of applying formal, informal and technical measures to mitigate the threats.

In theory, the study shall extensively describe threats originating both from the inside and outside and also reinforce the relatively new theories and approaches relating to the subject of insider threats, that is, effective management of information security threats requires both technical and non-technical solutions. The study will also add to the body of knowledge in information security studies by establishing the prevalent types of insider threats, mitigating strategies and challenges encountered controlling insider threats within commercial banks. This will be relevant to future studies in the field.

CHAPTER TWO

LITERATURE REVIEW

2.1The Concept of Insider Information Security

Information security, according to Brotby (2008), has imperatively become a matter for consideration at the highest organizational levels. Given the effects of fraud and data security breaches, it is no longer only a technical issue, but a business and governance challenge as well that involves risk management, reporting and accountability. Onthe subject of information systems and data security, the overwhelming majority of the available literature generally covers the technical aspects and specifically, the external threats more than the insider threats. The available literature on internal however has not failed to highlight this unbalanced approach to data security as one of the major reasons insider threats remain unchecked or unmitigated.

According to Brancik (2008), an insider is basically anyone who has similar access rights into a network, a system, or an application and therefore, an insider can be a current or former employee, a contractor, consultant, a software vendor, or a service provider. Probst, et al (2010) definition removes any technical or I.T. bias; "An insider is a person that has been legitimately empowered with the right to access, represent or decide about one or more assets of an organization's structure."

Insider Threat, according to Cole and Ring (2006), is anyone who possesses special access, rights, or knowledge with the intent to of causing harm or danger of any kind is considered an insider threat. If someone is entrusted with authorized access to a system and instead of fulfilling assigned responsibilities, manipulates a system to exploit it, they are considered an insider threat (Einwechter, 2002). Other descriptions postulate that the insider threats are basically the regular employees, contractors, and consultants who when joining or engaging with the organization are trusted and are given access to confidential resources of the company upon signing a non-disclosure agreement. Some of

them are however not skilled enough and may accidentally cause harm or expose the organization to external threats. Others take advantage of their accessibility and deliberately damage or steal confidential information. In either case, these individuals still fall under the 'insider threats' category (Aeran, 2006).Fraud**,** in the broadest of terms, can simply be defined as obtaining something of value or avoiding an obligation by means of deception and may embrace varied forms of conducts including corporate fraud that involves intricate planning and execution (Duffield andGrabosky, 2001).

2.2 Insider Information Security Threats

Identifying an inside attacker is a great challenge as Schultz (2008) highlights, to a great extent due to the approach of traditional strategies of information security. This is because much of their behavior in the course of an attack will superficially appear to be normal. Intrusion Detection Systems for instance would usually not issue alerts as they could constitute false alarms. Schultz (2002) further proposes that since many of the behaviors and activities of inside attackers are superficially innocuous, organizations should construct profiles for all the insiders. This includes employees, consultants, service providers, and contractors. Despite the potential impact in helping to identify inside attackers through use of such profiles, most organizations are generally hesitant when it comes to using them. Insider security threats may be one of the following types according to Aeran (2006).

Sabotage carried out with the chief aim of disrupting the organization's operations. A disgruntled employee may sabotage the organization's systems to take revenge. Theft involves stealing of the organizations intellectual property which is of commercial value. This could be information on computers, hardware, confidential documents, software code, customer records or financial data. Installation of malicious software code: software programs written with the sole aim of harming the organization's information systems. Examples include "time bombs" and "logic bombs". Viruses: harmful programs which have destructive payloads when executed. They are spread throughout the

organizations through E-mails, chats, information relays, file transfers, and removable drives. They may be activated deliberately or accidentally. Social engineering: the practice of obtaining confidential information through the manipulation of legitimate users. Social engineers trick employees into revealing sensitive information or having them do something that is against organization policy. Online adult activities: Adult and pornographic content are famous for propelling spywares and viruses. These online adult activities therefore make the information systems vulnerable to attacks. Installation of unauthorized software: software that are not installed by the I.T. department and can gather personal information of users and destroy data stored in computers. They include Trojan, spyware, and Key loggers.

Shaw, Post and Ruby (2005) infer that despite the studies and the analysis of the subjects who had committed the insider attacks, the characteristics pose serious management challenges. Information Technology professionals for and other individuals for instance may be honest and law abiding citizens and only commit these malicious acts when subjected to high levels of perceived personal or professional stress. However, they identified six personal characteristics with direct implications for risk: A history of personal and social frustrations, Computer dependency, Ethical flexibility, reduced loyalty, a sense of entitlement, and lack of empathy.

Increasing user awareness will reduce unintentional insider threats. This approach to information security as Rudolph et al (2002) argues will enhance detection of insider threats. They argue that employees who are aware of security concerns are able to prevent incidents. Employees can become detection instruments of the organization by familiarizing with the danger signals through awareness programs. Additionally, these employee awareness programs also have the advantage that they help develop positive effects on their attitudes and beliefs towards compliance with information system security policies (Bulgurcu et al., 2010, D'Arcy et al. 2009).

There are four types of Insiders according to Cole (2010): Pure Insider:an employee with all the rights and access that are associated with being employed. They can cause the greatest damage because they possess most of the access they need. Insider associate:someone with limited authorized access. They are not employees of the organization and do not require full access, but they do need limited access. Guards, cleaners, contractors, and third party service providers all fall in this category. Insider affiliates:Individuals who use the employee's credentials to gain access. This may be a friend, spouse, or client of the employee.Outside affiliates:Non-trusted outsiders who use open and vulnerabilities to gain access to organization's information resources, either virtually or physically.

According to Anderson (2012), to an average insider intent on causing harm or stealing data, the modern day office reads like an open book. While trends in threat models may be predictable, it is the insider threats and attacks that persist in exposing the "low-hanging fruit" or vulnerabilities in our office environments. Daily and simple exposures like, looking at a computer screen without authorization, are usually taken for granted and often lead to data leakages used in fraud. Capelli (2012) further implores that even as organizations become concerned about the malicious insider threats, they must also pay due attention to the emerging trends such as the malicious outsider taking advantage of the inadvertent insider.

In the banking and financial sectors, some studies such as one conducted by Randazzzo, Moore, et al (2004) has inferred that most incidences of fraud and insider attacks were not technically sophisticated. That is, they involved exploitation of the non-technical vulnerabilities such as basic business rules and organizational policies rather than vulnerabilities in the information system or network. Most incidents did not require technical wherewithal, further reiterating the importance of organizations to secure their data from the full range of users. That is, from system administrators, basic users responsible for data entry, employees offering support services, and even associates who provide services.

2.3Challenges in managing Insider Information Security Threats

A report on the trends of fraud in 2010 highlighted some of the types of threats facing banks as a result of Insider attacks. They included Chequefraud, card (ATM, Debit and Credit), Forgery, Wire Transfers, Counterfeiting, Identity theft, Embezzlement, and Loan Fraud among others. This means that the opportunities for Insider attacks have increased as the organizations' vulnerabilities are exploited as most of the fraud cases involve bank staffs (Kenya Bankers Association, 2010). Since an 'insider' possesses information, capabilities and knowledge not known to others like the external attackers, they are considered to be the chief challenge in securing information resources in the organization. The impact of the insider threats can occur in several dimensions such as financial loss, disruption to the organization's operations, loss of reputation, and even long term impacts on the organizational culture (Probst, et al, 2010).Cole and Ring (2006) report that, while not many executives will boldly admit that it is easier to trust your employees and keep life simple, than to suspect everyone and deal with the complexities it creates, the amount of losses corporations lose as a result of insider attacks might compel them to think differently.

According to Information security experts like Anderson (2012), new legislation has made it easier to prosecute and punish offenders. However, the chief challenge remains how to prevent the insider attacks. Because of the growing complexity of the attacks, most insiders are able to effectively cover their tracks and nearly impossible to detect.Probst, et al (2010) further explains that Insider behavior may be close to the expected behavior and therefore very difficult to distinguish. He notes that forensics tends to be highly undeveloped when it comes to addressing insider threats and still often the audit trails are generally insufficient.

According to Whitman (2004), acts of "human failure" or "errors" are one of the most severe threats to information security. Arguably the two most prevalent unintentional insider threats, user errors and negligence, expose the organization to external threats. Some of the underlying reasons normally attributed to user errors are; lack of experience

in using security tools, complexity of the security tools, and job stress due to time pressure and workload. On the other hand, although reasons behind negligence are complex, lack of awareness and motivation to use security tools due to their performance hindering characteristics can be considered as important factors. Thus, Whitman proposes to mitigate user error and negligence through five mechanisms: motivation, training, usability of security tools, time and workload pressure, and awareness.

Maxim (2012) argues that the insider threat today can range from the disgruntled employee with a technical capacity to embed an attack to a salesperson defecting to a competitor and bringing a price list with him. Organizations therefore need to realize the severity and the reality of the insider threat challenge. Careless or inadvertent actions also represent another significant insider threat vector. He further notes some of the macro trends that are aggravating the frequency and intensity of insider threats as:

Low data storage costs: The continuing drop in data storage costs means that it is often cheaper for organizations to store and archive all data rather than spending time examining it to determine what should be saved or deleted. The low storage costs means that data is always accessible, so if malicious insiders are looking for data, they can find it.Increased sophistication of attacks: Not surprisingly, individuals with technical acumen are often the ones committing insider attacks. If they have the skill to conduct the attack, it also means that they also likely possess the skills to cover up the theft, either by modifying/deleting log files or other actions. A Highly distributed work force: Today, employees are much more distributed and access data and applications over multiple channels (Wi-Fi, Ethernet and 3G) from multiple platforms (PC, smart phone, tablet, kiosk). Organizations need to support these multiple access methods to keep workers productive, but each new channel and platform introduces a new set of potential risks that must be managed. When other factors like cloud computing and outsourcing are factored in, the unfortunate reality is that data is essentially everywhere. Inadequate end-user awareness: Many employees simply lack knowledge of the organization's policies on information use as well as how data is to be used, shared and distributed. This can lead to actions such as users emailing confidential documents to a wide distribution.

These instances are not driven by malicious insiders but can be just as damaging to an organization as a malicious insider.

Organizations have attempted to combat the insider threat, but these approaches have generally focused only on detecting outright fraud - for example, controls are implemented to ensure proper segregation of duties within a financial application. Organizations seeking to mitigate insider threats face three other challenges. First, the sheer volume of audit and log data impedes forensics investigation and detection. Logging all IT activity is an important first step in combating insider attacks and today's highly distributed and complex IT environments generate massive volumes of logging data, but the sheer volume of data is very difficult to manage.

Secondly, most current approaches to addressing insider threats are reactive, not predictive. This helps immensely in forensic investigations, but the problem is that the attack or theft has already occurred. Therefore, organizations should be looking for solutions that can provide more analytic and predictive capabilities that if not able to prevent insider attacks, may still identify "at-risk insiders" and then implement more detailed logging on those individuals in response.

IT managers need to balance the risk of employees' need for additional access versus the lost productivity that would result if access was not granted to certain users. Many organizations also lack the necessary reporting tools to examine an individual's expanding entitlements over time which further compounds the problem. The result is that IT often struggles to answer the critical question, "Who has access to what?" confidently and accurately.

CERT (2009) posits that insider threats potentially pose the greatest harm to an organization. Since Insiders posses significant leverage over others who might want to

harm the organization, they can bypass both the physical and technical data security infrastructures designed to prevent unauthorized access. Most data security measures such as intrusion detection systems, electronic building access systems, and firewalls are primarily designed to mitigate external threats. Insiders are aware of their capabilities as well as their flaws and vulnerabilities and are therefore complicit in fraud and other data security breaches. Insiders will know how, when and where to attack and how to cover their tracks.

Brancik (2008) notes that information security and particularly, insider threat concerns will not typically evaporate over time and organizations cannot simply wait them out. They can evolve as has been seen from what may appear as an isolated problem to a systemic risk with enterprise-wide implications. The absence of an insider threat risk evaluation can for instance have a deleterious impact on the overall process of information security governance. This can in turn cause many negative consequences including an increased level of risk to the organization's operations, reputation, strategy, and finance. As Maxim (2012) proposes, organizations must come to task with the reality of the insider threat if they are to effectively mitigate the effects. Insider attacks are significant threat and are increasing in complexity. Organizations must confront the reality that nothing may completely prevent all insider attacks, but only those who adopt aggressive proactive approaches can help to reduce the risk.

2.4 Mitigations to Insider Information Security Threats

The challenge of data security in combating fraud is one of a complex and interdependent nature as James (1996) highlights. It must be approached comprehensively and all the elements that are interrelated considered. The human element for instance has further compounded the situation because of free will, they will always act in their best interests. According to Rudolph et al. (2002), Information security must now be seen as a people problem rather than the conventional technical approaches like sophisticated equipment and complex software solutions. The increasing numbers of breaches have proved this

fact, that is, an organization's security status is only as strong as the weakest link and if technological controls are not recognized by users, information systems will be compromised.

Aeran (2006) suggests that an understanding of the motivations for the insider attacks will also aid in establishing key characteristics of the Insiders if not help in averting the attacks altogether. The following factors may motivate the insiders to carry out attacks either independently or as a combination: Financial gain, disgruntlement, espionage, Revenge, curiosity and quest for a challenge, emotional distress and desire for respect, decision failures, and mental disorders.

2.4.1 Non-technical approaches to mitigations

It is just as critical to pay due attention to the non-technical factors that motivate the various kinds of insider attacks and pose a potential threat. Social studies take us back to the same predictable sources of delinquent acts according to Hirschi, (1969). He postulated for instance that when an individual's bond to society is weak or broken, delinquent acts are usually the results. Hollinger (1986) reported that production and property defiance is many times more likely when an individual's attachment to an organization is low. Stanton et al. (2003) investigated the relation between organizational commitment and information security and reported that individuals with high organizational commitment are less likely to have behaviors that may put their company at risk. These theories and approaches can help the firm in detecting and mitigating insider threats.

One of the most striking findings on the insider threat issue has generally been the unsophisticated nature of majority of insider attacks. Researchers and experts like Keeney et al (2005) have confirmed through studies that majority of the incidents used technically unsophisticated methods of attack like user commands, information

exchanges and exploitation of the physical security vulnerabilities in the organizations. And since majority of insider attackers have a low level of technical and I.T. skills and use relatively simple 'trade craft' to achieve their goals, it is even more challenging for organizations to protect themselves. This dispels the prevailing myths and approaches that all attacks by malicious insiders are carried out by sophisticated operators.

Although studied extensively, the Socio-behavioral side of insider threats is often neglected in the security policy context as highlighted by Barman (2002) and Kabay (2002). They note that security policies approaches are conventionally associated with physical security, network security, and Internet and e-mail security. However these policies should also incorporate different behavioral and psychological aspects of insider threats.

According to Cole and Ring (2006), any approach to dealing with mitigating the Insider attack problem must begin at the hiring stage. Organizations generally work under the assumption that once they hire an employee or a contractor, that person automatically becomes part of a trusted group of people. Many organizations perform no reference or background checks and as long as the hiring manager likes them, they will hire them. Many of such people might not be who you think they are and the lack of a proper validation can be a costly one if not a fatal blunder. Cole and Ring introduces a highly probable scenario: "Because many organizations, in essence, hire complete strangers who are really unknown entities and give them access to sensitive data, the insider threat is something that all organizations must worry about. If a competitor or similar entity wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to find a job opening, prep someone to ace the interview, have that person get hired, and they are in. The fact that it is that easy should scare you. Many companies have jobs open for several weeks and it could take a couple of weeks to set up an interview. That gives a competitor focused on your company a four-week period to prep someone to ace an interview.

2.4.2 Technical approaches to mitigation of Insider Information Security Threats

Technology-based control mechanisms will reduce intentional insider threats to the information security level. Haugen andSelin (1999) point out some of the most common technology based preventive controls as passwords, firewalls, connection security, and cryptography. Sandhu (2002) argues that password-based authentication is one of the persuasive technologies that can be implemented as a control mechanism. He further postulates that though they are not as secure as biometric systems, they can be strengthened so as to be used for the less critical processes within the organization.

Brussin (2002) states that, as with passwords, firewalls have become one of the most conspicuous security technologies used in many organizations. Einwetcher (2002) points out that, intrusion detection systems are also considered as effective detective controls since they are not only used to detect attacks, but also identify and analyze attack trends. According to Chokhani (2002) and Bace (2002), some of the more advanced technology based controls that can be implemented are public key infrastructures, certificate authorities and vulnerability assessments.

Previous studies on insider information security threats have highlighted the various types of insider attack, forms of insider threats and various types of insiders. Substantial studies contributing to insights in the field has provided the characteristics and trends of insiders and clarity on the behaviors to watch. In mitigating insider information security threats, though several approaches have been suggested, strategies in mitigation insider threats still remains elusive , hence the basis of predicting and monitoring the potential activities leading to the vice and control approaches leaves room for more investigations to be done.

In the Kenyan banking sector, knowledge of the prevalent type of insider threats will be essential to enable the banks to focus more on controlling the consequences of insider attacks.

Technological advances embraced by Kenyan banks continue to open up more opportunities for insider attacks. Comprehensive solutions should now be sought to address Information Security concerns like the Insider attacks. This will involve both technical and non-technical mitigation strategies.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1Research Design

This study made use of the survey research design model. Surveys are more flexible in the sense that a wider range of information can be collected. They provide information that is useful for drawing comparisons and generalizations.This section comprised the research design that was employed on the study, the population and its description, data collection, analysis and the procedures.

3.2 Population of the study

The study was conducted on all the 43 commercial banks in Kenya and the questionnaires were distributed to selected representatives. A Census approach was used and all the representatives of the entire population (the respondents) were targeted.The questionnairesresponses were handled with utmost confidentiality.

3.3Data Collection

The data was collected through the use of structured questionnaires, IT managers or Information Security managers were requested to fill in the questionnaires which contained both closed and open-ended questions to extract accurate information from the respondents.

The questionnaire had three sections; Section A which covered the respondent's background, Section B which covered the types of Insider Threats, and Section C which covered mitigation strategies employed by the commercial banks in Kenya.

A “drop-and-pick latter” approach was employedin administering the questionnaire and helping the researcherin assisting the respondents in case of any issues in filling the questionnaires and to ensure maximum or high response rates.

The questionnaires underwent a test run to ensure effective data capture and reliability before the official roll out.

3.4Data Analysis

On receiving back the questionnaires from the respondents, the data was checked to ensure completeness and uniformity. The data was then coded and tabulated to facilitate data analysis and subjected to various analyses.

Data collected helpedin analyzing the nature, type and frequency of insider threats in the population under study. Data from Section A andB of the questionnaire concernedrespondents’ background and types of insider threats. Descriptive statistic such as mean scores, standard deviation, percentages and cumulative frequency were used to analyze the data. As for data which relates to Section C of the questionnaire, analysis of risk mitigation strategies was done usingmulti- variants statistical techniques such as factor analysis to rank the mitigation strategies in order of suitability.

CHAPTER FOUR

DATA ANALYSIS, INTERPRETATIONS AND DISCUSSIONS

4.1 Introduction

The reporting in this chapter is in relation to two research objectives. These research objectives are: To determine the nature of Insider Threats facing Commercial Banks in Kenya and to determine mitigation strategies which commercial banks could use to manage insider information threats.The chapter offers a detailed report on the analysis of the primary data collected from thequestionnaires, their presentation, interpretation and discussions of the findings. Statistical methods which included mean, standard deviation and factor analysis were used.

This Chapter is divided into three sections: Section One which relates to demographic information of the population, Section Two which focuses on types and nature of Insider threats facing commercial banks in Kenya and Section Three which covers the mitigation strategies. There were a total of 31 respondents who represented a total of 31 different commercial banks out of the available 43 commercial banks as at the time of the research. The study covered 72% of the population under research, and has the double benefit of enhanced credibility of the findings and reinforced conclusions.

4.2 Demographic Information

Analysis of demographic data was done and from the questionnaires respondents gave their personal details like Gender, Age, position and duration of their services. Data which related to the organization such as number of branches, ownership structure, period of operation, size of the organization and number of staff in the banks. These details were essential in providing the background for both the respondents and banks under study.

4.2.1 Gender of the respondents

Table 4.1Gender

Gender	Percentage	Frequency
Female	0	0
Male	100	31
Total	**100**	**31**

Data on gender were collected from the 31 respondents, the data was analyzed and the outcomes were as presented as percentages in Table 4.1. Interestingly the respondents were all male.

This signals the gender distribution in the field of information security as seen from the banking industry perspective alone. This information may be useful in drawing conclusions about the gender distribution in the field of information technology in a general sense.

4.2.2 Age of the Respondents

Table 4.2 Respondents Age

Age bracket	Percentage	Frequency
Below 25	-	-
25 - 30	16	5
31 – 35	41	13
36 – 40	20	6
41 - 45	13	4
Above 46	10	3
TOTAL	**100**	**31**

Data related to the age of the respondents was collected and tabulated as presented on Table 4.2. The highest number of Information security professionals in commercial banks is 31-40 years old having a representative of 61% . Only 10% were above the age of 46

and majority of them were below 40 years. Coincidentally, the average age of the perpetrators of insider attacks falls in the 25-35 year old category as also seen in Table 4.13. The findings reflect similarity between the staff dedicated with managing the security and perpetrators are within the same age group.

4.2.3 Position of the Respondents

Table 4.3Position of the Respondents

Position/designation	**Percentage**	**Frequency**
I.T manager	48	15
Chief information officer [CIO]	6	2
Chief information security officer[CISO]	10	3
I.T. Consultant	26	8
Others	10	3
TOTAL	**100**	**31**

Data on respondent's designations was collected and analyzed as presented in Table 4.3. Information Technology manager traditionally holds the responsibility of information security in most of the commercial banks with the highest rate of 48% of the respondents. 26% of the banks have engaged the services of consultants in information security. These are usually experts in the field of information security. 10% of the respondentshave security team with clear roles of information security planning and monitoring to ensure the banks system is well secured. This is a good development though with the current trends of security incidents, banks should mature towards dedicating security skilled teams to manage the role.10% have the role of security being managed by other departments' e.g. Risk, Audit or Compliance teams.

4.2.4 Duration of Work

Table 4.4 Amount of Time Worked In the Organization

Duration worked [years]	Percentage	Frequency
Below 5	78	24
6 – 10	15	5
11 – 15	7	2
16 – 20	-	-
Over 20	-	-
Total	**100**	**31**

Data in relation to the period in which the respondents have been with the bank was collected and tabulated as in Table 4.4. Information security officers are generally engaged in one organization for less than 5 years. 78% of the respondents were engaged with the organization for less than 5 years and only 15% of them were engaged with the organization for a period of up to 10 years. This is related to the average age of entry into the field as shown in Table 4.2but may also signal a high rate of employee turnover either in the banking industry or in the field of information security.

It is important to note the turnover frequency is also high because of the consultants acting as information officers having their contracts/consultancy expiring.

4.2.5 Duration of the organizations' operation

Data relating to the period of operation was collected and the analysis presented in Table 4.5. 45%nearly half of the respondents have been in operation for over 20 years. However, the banking industry has seen significant growth through relatively new entrants as reflected from the study. 33% of the respondents have been in operation for not more than 5 years. Overall, this means that most of the banks have been privy to or even been victims of the exponential increase in the number and frequency of insider attacks in the last few years.

Table 4.5Organization's Duration in Operation

Organization's duration in operation [years]	Percentage	Frequency
Below 5	33	10
6 – 10	11	4
11 – 15	4	1
16 – 20	7	2
over 20	45	14
Total	**100**	**31**

4.2.6 Ownership

Table 4.6 Ownership

current shareholding structure	percentage	frequency
Locally owned institution	42	13
Government-controlled majority shares	11	4
Foreign owned but locally incorporated	17	5
Foreign owned NOT locally incorporated	10	3
Owned by both locals and foreigners	20	6
Other	-	-
Total	**100**	**31**

Data on bank's ownership was collected at presented in Table 4.6. The ownership of commercial banks in Kenya is mostly local followed by ownership by both local and foreign partners. These two categories comprised 62% of the total respondents. However, 17% of the organizations under study were foreign-owned but locally incorporated while 11% had a major government influence in their shareholding.

4.2.7 The size of the organization

Table 4.7 Size of the Organization

Size of bank in terms of total asset value [ksh]	Percentage	Frequency
Below 5 Billion	26	8
5 – 20 Billion	34	10
20 – 50 Billion	12	4
50 – 100 Billion	15	5
100 – 200 Billion	6	2
Above 200 Billion	7	2
Total	**100**	**31**

Data collected on size of the banks with asset value as the measure was collected and presented in Table 4.7. Most of the commercial banks with 60% representation had an asset base of up to Ksh. 20 Billion as at the research period and only 13% of them had an asset base of more than Ksh. 100 Billion. This is a good indication of the seriousness Bank shareholders have invested hence the high expectations of returns. High level security will be of paramount importance in safeguarding value of the assets. Since data is critical to the organization, banks have resources at their disposal which could be utilized to secure data.

4.2.8 Number of Employees

Table 4.8 Number of Employees

Number of Employees	Percentage	Frequency
Below 100	15	5
101 – 500	55	17
501 – 1000	15	5
1001 – 5001	15	4
Above 5000	-	-
Total	**100**	**31**

Data in relation to the number of employees within the banks was collected and tabulated in Table 4.8. More than 55% of the respondents have between 100 and 500 employees while 15% of the respondents have more than 1, 000 employees. 15% of them had fewer employees, less than 100 employees. The number of staff is crucial in determining the scope of the management, segregation of duties, policies and training required in preventing insider threats. This reflects a substantial growth in bank's staff numbers perhaps due to the massive expansions by banks in remote areas to bring the services to the customers.

4.2.9 Number of branches in Kenya

Table 4.9 Branches in Kenya

No. of branches in Kenya	Percentage	Frequency
Below 10	17	5
11 – 30	48	15
31 – 50	25	8
51 – 70	-	-
71 – 100	-	-
Above 100	10	3
Total	**100**	**31**

Data on number of branches owned by the banks in Kenya were collected and represented in Table 4.9. Nearly half(48%) of the banks under study have between 11 and 30 branches spread around the country while 10% of them have more than 100 branches across the country. 17% of the organizations had less number of branches, fewer than 10. The premium on information security increases with the dispersion of the banks' operations as 73% of the banks under research had each between 10 and 50 branches spread across the country.The growth of the number of branches by banks has the benefit of availing the banking services to customers' convenience, this being key in bringing the services closer to the customers, it also increases the avenues for attacks by malicious insiders.

4.3 Types of Insider Threats

Table 4.10Nature of Threats Faced [% values]

Insider Threats	No Extent at All	Little Extent	Moderate Extent	Great Extent	Very Great Extent	Mean	Std. deviation
Sabotage (disrupting operations)	66	21	13			1.47	0.288
Theft (stealing information)	20	17	47	16		2.59	0.550
Spoofing (pretending to be something or someone that one is not)	73	18	9			1.36	0.302
Viruses		33	56		11	2.89	0.687
Social engineering (manipulation of users to obtain information)	38	31	24	7		2	0.285
Installation of unauthorized software	20	51	18	8	3	2.23	0.354
Hacking (accesses a computer system by circumventing its security system)	58	35		7		1.56	0.323
Purposefully installing malicious software	63	21	16			1.53	0.290
Impersonation of other users	50	35	12	3		1.68	0.283
Physical security breaches	44	26	30			1.86	0.381
Tampering with data (unauthorized changes of data or records)	44	19	15		22	2.37	0.396
Unauthorized Access	33	56	4	7		1.85	0.439
Destruction of critical data	59	41				1.41	0.395
Denial of service attacks	79	14	7			1.28	0.324
Organized Crime	61	21	14	4		1.61	0.241

(Insiders colluding with criminal gangs)							
Identity Thieves (Impersonation Fraudsters)	71		18	11		1.69	0.323
Activists (to bring social or political change through actions)	78	19	3			1.25	0.335
Password Cracking	74	22	4			1.3	0.323
Phishing (acquiring information and/or money from people without their knowledge)	70	22	8			1.38	0.300
Key loggers (hardware or software-based, they capture keystrokes)	54	36	10			1.56	0.321
Selling employer's confidential information to the competitor(s)	68	25	7			1.39	0.304
Others *[Specify and Rate accordingly]*							

Some of the insider threats had little impact to the organizations under research as they were not experienced by most of them. They include Hacking (accesses a computer system by circumventing its security system), Purposefully installing malicious software, Physical security breaches, Destruction of critical data, Selling employer's confidential information to the competitor(s), Password Cracking, Identity Thieves (Impersonation Fraudsters), Organized Crime (Insiders colluding with criminal gangs) and Sabotage (disrupting operations). This may be due to the rate at which the banks have employed structured defense mechanisms and the tracking and securing of their physical environments.

To consolidate and give presentation of the data, the study utilized the statistical functions of mean and standard deviation. The mean represents the average rating of all

the respondents to the particular practice while the corresponding standard deviation shows the spread of the ratings (how far or the range within which the individual ratings are from the mean rating).

In Table 4.10, the means range from 1.25 the lowest to 2.89 the greatest mean of 2.89 is closer to 3, which is moderate and mean of 1.25.is closer to 1 meaning no extent at all. Using the mean values, theft,virus, installation of unauthorized software and tampering with data had a score of more than two, hence on average banks have encountered insider threats through such approaches.Notably, stealing of information and viruses were experienced in moderate extents in 47% and 56% of the organizations respectively. With standard deviations of less than one (1), the response's distribution is spread very closely around the mean response allowing for accurate conclusions and inferences.

4.3.2 Characteristics of Insiders

Table 4.11Characteristics of Insiders [percentage values]

Characteristics	No Extent at All	Little Extent	Moderate Extent	Great Extent	Very Great Extent	Mean	Std. deviation
Have Criminal tendencies	30	46	15	8		1.99	0.335
Have a reduced sense of loyalty	22	30	37	11		2.37	0.422
Social transgression tendencies	43	36	15	6		1.84	0.268
High ethical flexibility	33	41	15	11		2.04	0.294
Emotional distress	48	32	20			1.72	0.319
Resistance to authority	59	26		15		1.71	0.314
Lack of empathy (disregard for the impact of other peoples actions)	65	15	12		9	1.76	0.237
Introversion(often loners)	56	26	18			1.62	0.296
Mostly depressed	64	20	16			1.52	0.291
Frustration with the workplace	44	28	28			1.84	0.366
Across system usage patterns (Unusual system usage patterns)	46	33	17		4	1.83	0.263
Making of Meaningful errors	65	23		12		1.59	0.300
Deliberate markers (leave small, intentional signs)	56	30	14			1.58	0.296
Weakness in handling conflicts	68	20	12			1.44	0.290
Curiosity to learn systems both operations and technical	46	31	19	4		1.81	0.270
Have Tendencies to work extended hours and preferably late	27	38	23		12	2.32	0.320

nights and weekends							
Obsessive tendencies (continuously pre-occupied)	65	12	23			1.58	0.338
Imitation and modeling those whom they respect	67	8	25			1.58	0.367
Others *[Specify and Rate accordingly]*							

To varying extents, across system usage partners, tendencies to work extended hours, late night and weekends, high ethical flexibility, curiosity to learn the system, social transgression tendencies, among other characteristics have a seeming prevalence in insiders. As seen from the distribution of responses (mean and standard deviations), the responses are closer to the mean. This means most of the organizations are closer to conclusive agreements about the particular characteristics they were rating.

A reduced sense of loyalty is the most prevalent characteristic of the insider according to the study. As attested by 78% percent of the respondents, it is prevalent from a moderate extent to a very great extent in those banks. This is similarly followed to the same extents by tendencies for working long hours till late at night and weekends as established in 73% of the banks under research.

4.3.3 Types of insiders

Table 4.12Types of Insiders

Types of Insiders	No Extent at All	Little Extent	Moderate Extent	Great Extent	Very Great Extent	Mean	Std. deviation
Pure Insider [*employee with all rights and access*]	7	15	44	34	-	3.05	0.676
Insider associate [*guards, cleaners, contractors, service providers*]	48	30	15	17	-	2.21	0.264
Insider affiliate [*friend, spouse, client who uses employee credentials*]	74	22	4	-	-	1.3	0.323
Outside affiliate [*outsiders who use open access and vulnerabilities*]	77	15	4		4	1.39	0.296
Others *[Specify and Rate accordingly]*	2	-	-	1	-	0.06	0.018

Employees with all rights and access within the organization, the pure insiders, are in varying degrees responsible for majority of the insider attacks according to 93% of the organizations, with 34% of the organizations citing their danger to a great extent. The

insider affiliates and outside affiliates are yet to be encountered out of the 4 types of insiders in 74% and 77% of the organizations respectively.

In Table 4.12, the means range from 0.06 the lowest to 3.07 the greatest mean of 3.07 is above three, which is moving from moderate to great extent and mean of 0.06 is lower than one meaning no extent at all. This confirms that by using the mean values, pure insiders as the most prevalent type of insider threat with the highest mean of 3.05.

Sample distribution as far as the various categories was concern, the standard deviation is higher in pure insiders, portraying the diversity within the sample considered.

4.3.4 Average age of perpetrators encountered

As shown in Table 4.13, more than half the perpetrators of insider attacks encountered by the banks are aged between 25 and 30 years old 57% and 25% of them were in the 31 – 35 year category. It is outside the scope of this research study to draw conclusions or insights into the relationship between certain age-groups and insider attacks. However, insider attackers the results show range from as young as 25 years according to 14% of the organizations while there are yet to be recorded cases of perpetrators who are above 40 years of age.

Table 4.13 Average Age of Perpetrators Encountered

Average age of perpetrators	**Percentage**	**Frequency**
Below 25	14	4
25 – 30	57	18
31 – 35	25	8
36 – 40	4	1
41 – 45	-	-
46 and above	-	-
TOTAL	**100**	**31**

4.3.5 Motivations for insider attacks

Table 4.14 Motivations for Insider Attacks

Motivations	No Extent at All	Little Extent	Moderate Extent	Great Extent	Very Great Extent	Mean	Std. deviation
Financial gain–(stealing or manipulating financial details for personal monetary benefits)	11		22	11	56	4.01	1.147
Disgruntlement (Frustrated employee will think of harming the company).	11	39	39	11		2.5	0.483
Espionage (spy or mole that is influenced by criminals or competitors targeting the bank)	54	15	15	7	9	2.02	0.111
Quest for challenge (explore the world around or take it as a challenge)	41	24	35			1.94	0.433
Revenge (employees with negative feelings towards the company or individuals within the company)	60	24	16			1.56	0.289
Desire for respect (Employees desiring to proof themselves because they are less skilled than others)	87	5	4	4		1.25	0.352
Emotional distress (Employee is highly frustrated)	56	20	24			1.68	0.327
Sabotage (disruption of company operations)	67	25	8			1.41	0.300
Theft (data stored in computer hardware and software, company or customer financial data)	57	8	25			1.48	0.345
Curiosity (experimenting with company's network resulting in disruption of services)	56	44				1.44	0.410

Hooliganism (such as defacing a Web site)	68	28	4			1.36	0.324
General malice	76	16	10			1.38	0.312
Politics (internally or externally instigated)	75	17	8			1.33	0.309
Challenge security professionals	70	30				1.3	0.358
Others *[Specify and Rate accordingly]*							

Financial gain is considered one of the greatest motivations for insider attacks with 56% of the organizations under research ranking it as very great extent. Also using the mean, the experience has been above average.It has the highest distribution as seen from the standard deviation though it is rated highest by more than half of the total respondents. Through a prevalent and traditional motivation, financial gain is in itself the greatest motivation as seen from the study. Just over half of the total respondents cited it to very great extent. 11% of the respondents have in their experience at the time of research, not found it as a motivation for insider attacks.Same results are confirmed when using the mean values; the highest mean was 4.01, which is above great extent.

According to the respondents, a disgruntled or frustrated employee and those seeking for a challenge account for 39% and 35% respectively, to a moderate extent, be motivated to carry out an insider attack. However, general malice, hooliganism, internally or externally instigated politics, desire for respect, challenging security professionals and revenge are considered as moderate motivations for insider attacks according to the respondents. However, 30% of the respondents noted that to a little extent, insiders are motivated by the thrill of challenging the information security professionals.

4.4 Mitigation strategies

Table 4.15The Mitigation Strategies Employed

Mitigation Strategies	No Extent at All	Little Extent	Moderate Extent	Great Extent	Very Great Extent	Mean	Std. deviation
Screening of applicants during recruitment			30	20	50	4.2	1.021
Consistently enforcing of policies and controls		15	33	15	37	3.74	0.717
Instituting periodic security awareness training for all employees		24	40	28	8	3.2	0.509
Use of data encryption	15	11	32	14	26	3.19	0.490
Use of Structured defense against remote attacks (e.g. Installation of firewalls)				30	70	4.7	1.522
Regular vulnerability assessments	8	27	12	38	25	3.75	0.610
Stringent Service Level Agreements with third party	15	25	36	12	7	2.56	0.347

service providers							
Strengthening of Internal controls and monitoring of information system transactions			32	48	20	3.88	0.806
Regular review of information security processes, policies and standards		8	40	36	16	3.6	0.630
Implementing strict password and account management policies and practices.			54	19	27	3.73	0.749
Anticipation and management of negative workplace issues	16	44	28	12		2.36	0.394
Role Based Access Control and/or Dual Access control	20	10	10	30	30	3.4	0.622
Enforcement of separation of duties and least privilege		31	19	38	13	3.36	0.544
Use of Data Loss Prevention suites	20	4	36	16	24	3.2	0.504

(e.g. Restrictions on removal media like flash disks, CDs, etc.)							
Implementing secure backup and recovery processes		15	46	27	22	3.86	0.590
Logging and monitoring employee online actions		33	33	23	11	3.12	0.393
Implementing system change controls		8	54	15	25	3.63	0.696
Tracking and securing of the physical environment (e.g. use biometric systems)	4		40	16	40	3.88	0.843
Use extra caution with system administrators and technical or privileged users		22	26	19	33	3.63	0.606
Developing an insider incident response plan	44	15	11	22	8	2.35	0.236

Monitoring and responding to suspicious or disruptive behavior of employees.	11	26	33	22	8	2.9	0.359
Deactivating computer access following staff termination		10	10	38	41	4.07	0.912
Considering insider threats in the software development life cycle	27	19	35	12	7	2.53	0.313
Warning of all staff to be alert to anyone asking for sensitive or restricted information	27	12	19	27	15	2.91	0.350
Establishing a formal grievance procedure for staff to vent their feelings	48	14	21	17		2.07	0.279
Setting up an easy and confidential system for staff to report any abnormal behavior from their colleagues	43	21	25	11		2.04	0.267

Half of the total respondents perform screening of applicants to a very great extent and a further 20% employing it to a great extent while the remaining batch employs it moderately. Notably, 44% of the total respondents do not have in place an insider attack response plan while 43% lack a proper system for easy and confidential reporting of any abnormal behavior from their colleagues. Nearly half 48% of the organizations under research do not have a formal or organized grievance procedure for staff members to vent their feelings or seek redress.According to the data collected, all the banks employ regular review of information security processes, policies and standards. They also carry out strengthening of internal controls and monitoring of information system transactions in varying extents. Implementation of role based access was observed in 80% of the banks while all of them carry out monitoring in varying degrees of their employees' online activities and system alterations.Most of the organizations 70% employ structured defense applications and equipment against remote attacks. This includes installation of firewalls among other applications as it was also observed that all they implement secure backup and recovery processes.

In Table 4.15, the means range from 0.06 the lowest to 3.07 the greatest mean of 4.7 is above 4, which is moving from great extent to very great extentand lowest mean of 2.04 is lower than 2 meaning little extent. These results confirm that banks at least have employed the mitigating strategies available in an effort to control insider threats. It is imperative that the insider threat poses a big challenge to banks.

4.4.2 Challenges Faced

Table 4.16 Challenges Faced

Challenges	No Extent at All	Little Extent	Moderate Extent	Great Extent	Very Great Extent	Mean	Std. deviation
High costs of acquiring, licensing			39	29	32	3.93	0.739

andmaintaining the security solutions.							
Lack of technical experience in using security tools	11	15	19	30	25	3.43	0.519
Lack of knowledge on the banks policies on information use	15	27	58			2.43	0.735
Difficulty in achieving clear staff background screening	8	36	40		16	2.8	0.509
Lack of staff security training	7	48	30	15		2.53	0.452
Vendor/Contractor management Issues	12	44	32	12		2.44	0.433
Poor Communication flow within the organization	12	16	40	32		2.92	0.610
Insufficient Audit trails	7	15	33	11	34	3.5	0.654
Technology advancement increasing opportunities for insiders	8	16	24	52		3.2	0.852
Complexity of the security tools	7	18	37	7	31	3.37	0.628
Job stress due to workload pressure	11	22	44	11	12	2.91	0.449

The technological advances are increasing more opportunities for insider attackers according to more than half52% of the banks to a great extent. To a little extent, the lack of staff security training is noted as a challenge by nearly half 48% of the banks and to a moderate extent, the lack of knowledge of the bank's policies on information use in 58% of the banks. Lack of technical experience and knowledge in using information security tools was to a great and very great extent a significant challenge to more than half of the respondents 55%. Complexity of the information security tools is, to a moderate extent, a challenge to more than a third 37% of the banks under this study.Poor communication flow is to a moderate extent also cited by 40% of the banks as a challenge in relation to information security. An additional 32% cited to a great extent poor communication flow as a challenge.

In varying degrees moderately – very great extents, all the banks under this study are challenged by the high costs associated with the acquisition, licensing and maintenance of the various information security solutions. This is considering the single most prevalent, and to a great extent, mitigation strategy as seen in table 4.15 is the employment of structured defenses such as firewalls. Though all the banks perform screening of employees, only 8% of them have not encountered challenges in achieving clear background checks although ascertaining the methods and facts of the checks still requires more research.The study found out that in varying degrees, moderate to very great extents, the lack of proper and sufficient audit trails is a challenge to many of the organizations under the study 78%.

The mean and standard deviations conclude that organizations face most of these challenges to some extents. This is seen from the fact that the lowest mean rating is 2.43 considering all the challenges. With a 3.93 mean rating and a 0.739 standard deviation, high costs associated with acquiring, licensing, and maintaining security solutions is the most prevalent challenge according to the respondents.

4.5 Research Objectives

The first objective of this research study was to determine the nature of Insider Threats facing Commercial Banks in Kenya. The research concluded from the findings that all the listed kinds of information security were experienced in the banks to some extents as shown in Table 4.10. Identity thieves were not experienced by any of the respondents while viruses and stealing of the information were the most common threats experienced. Up until the potential or actual danger is obvious, detecting insider attacks is a difficult and often elusive task (Schultz, 2002). This is also seen from the study in that; the types of threats are sporadic see Table 4.10. However, stealing of information is experienced moderately in more than half of the banks according to the study. 47% of the banks have to deal with viruses and other malware to a moderate extent.

The traditional reactive approaches make it difficult to detect and so predictive models have been proposed such as characteristics and behaviors of insiders (Schultz, 2002). Table 4.11 highlights certain characteristics that are common in the banks. Tendencies to work long and extended hours, high ethical flexibility, social transgression tendencies, across system usage patterns and a heightened curiosity to learn about the information systems were cited as common characteristics of the insiders according to their banks' experiences. The greatest indicators according to the respondents are working long and extended hours (even weekends and holidays) and a reduced sense of loyalty. This was noted by at 73% and 78% of the total respondents respectively.

These characteristics and behavior may be close to the expected behavior in the employees and may be quite a challenge in distinguishing it (Probst, et al, 2010). Because of insufficient audit trails or underdeveloped forensics, business leaders therefore will readily admit that it is easier to trust the employees and keep it simple, rather than be suspicious of everyone and have to deal with the complexities it creates (Cole and Ring, 2006). Nevertheless, an understanding of the motivations for the insider attacks is critical as it will form a useful basis for establishing key characteristics of the insiders. If not

helping in averting the insider attacks altogether, this understanding is crucial in constructing the elusive Insider profile (Aeran, 2006).

As a result, the pure insiders, that is, the employees with full access, pose the greatest threat according to most of the banks. 93% of the banks in various extents cited the pure insider as the most common threat in their experience. The outside affiliates and the insider affiliates are less prevalent and are yet to be encountered by 77% and 74% of the banks respectively. This may be because all the banks according to the study employ structured defense mechanisms firewalls and antispyware/malware.

The second objective was to determine mitigation strategies which commercial banks use and could employ to manage insider information threats. There was a notable trend with nearly half of them lacked both an insider incident response plan and a confidential system for staff to report abnormal behavior among colleagues (44% and 43% of the respondents). This means they may be missing out on the potential benefits of accountability and the ability to minimize damage in case of an attack.

Screening of applicants was one of the most widely employed according to the study, with all the banks making use of it to, at least, moderate extents. However, the effectiveness of this strategy may be questionable as only 8% of the respondents did not record any challenges as far as it is concerned while an overwhelming majority 92% to varying degrees consider it a challenge.

Further, nearly all the banks consider the complexity of the security tools and the mitigation strategies as a challenge 93%. This may hamper the adoption of these tools and strategies and may the wide gap between the great advances in technical countermeasures and the fact that we are not any less vulnerable to data security breaches (Schmidt, 2011). All the banks, according to the study, perform regular review of

information security processes, policies and standards. They also perform strengthening of internal controls and monitor information system transactions. All of the banks monitor their employees' online activities and employ structured defense mechanisms like anti-virus software and firewalls.

4.6 Factor Analysis - Mitigation Strategies Employed

The factor analysis carried out was to reduce data into key information that was to guide in as a method of data reduction. It does this by seeking unobservable (latent) variables that are reflected in the observed variables (manifest variables).

4.6.1 Mitigation strategies employed

Table 4.17 Factors - Mitigation Strategies Employed

F1	Screening of applicants during recruitment
F2	Consistently enforcing of policies and controls
F3	Instituting periodic security awareness training for all employees
F4	Use of data encryption
F5	Use of Structured defense against remote attacks (e.g. Installation of firewalls)
F6	Regular vulnerability assessments
F7	Stringent Service Level Agreements with third party service providers
F8	Strengthening of Internal controls and monitoring of information system transactions
F9	Regular review of information security processes, policies and standards
F10	Implementing strict password and account management policies and practices.
F11	Anticipation and management of negative workplace issues
F12	Role Based Access Control and/or Dual Access control
F13	Enforcement of separation of duties and least privilege
F14	Use of Data Loss Prevention suites
F15	Implementing secure backup and recovery processes
F16	Logging and monitoring employee online actions
F17	Implementing system change controls
F18	Tracking and securing of the physical environment (e.g. use biometric systems)
F19	Use extra caution with system administrators and technical or privileged users
F20	Developing an insider incident response plan
F21	Monitoring and responding to suspicious or disruptive behavior of employees.

F22	Deactivating computer access following staff termination
F23	Considering insider threats in the software development life cycle
F24	Warning of all staff to be alert to anyone asking for sensitive or restricted information
F25	Establishing a formal grievance procedure for staff to vent their feelings
F26	Setting up an easy and confidential system for staff to report any abnormal behavior from their colleagues

The above variables are some of the anticipated mitigation strategies employed in mitigating information security threats among commercial banks in Kenya.

4.6.2 Correlation

Table 4.18 Correlation Matrix

Factors	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	F13	F14	F15	F16	F17	F18	F19	F20	F21	F22	F23	F24	F25	F26
F1	1.000	-.079	-.069	.365	.104	.269	.033	.047	-.098	.162	.113	.035	1.000	-.079	-.069	.365	.104	.269	.033	.047	-.098	.162	.113	.035	.104	.269
F2	-.079	1.000	.006	-.095	-.119	-.009	-.006	-.025	-.028	-.095	-.123	.000	-.079	1.000	.006	-.095	-.119	-.009	-.006	-.025	-.028	-.095	-.123	.000	-.119	-.009
F3	-.069	.006	1.000	.032	-.002	.002	-.014	-.011	.991	.000	-.024	-.027	-.069	.006	1.000	.032	-.002	.002	-.014	-.011	.991	.000	-.024	-.027	-.002	.002
F4	.365	-.095	.032	1.000	.438	.331	.022	.167	.025	.086	.078	.023	.365	-.095	.032	1.000	.438	.331	.022	.167	.025	.086	.078	.023	.438	.331
F5	.104	-.119	-.002	.438	1.000	-.056	.013	.159	.026	.172	.069	.033	.104	-.119	-.002	.438	1.000	-.056	.013	.159	.026	.172	.069	.033	1.000	-.056
F6	.269	-.009	.002	.331	-.056	1.000	-.013	-.013	-.033	-.035	.100	-.023	.269	-.009	.002	.331	-.056	1.000	-.013	-.013	-.033	-.035	.100	-.023	-.056	1.000
F7	.033	-.006	-.014	.022	.013	-.013	1.000	-.002	-.015	.135	.007	.706	.033	-.006	-.014	.022	.013	-.013	1.000	-.002	-.015	.135	.007	.706	.013	-.013
F8	.047	-.025	-.011	.167	.159	-.013	-.002	1.000	.007	.011	-.007	-.011	.047	-.025	-.011	.167	.159	-.013	-.002	1.000	.007	.011	-.007	-.011	.159	-.013
F9	-.098	-.028	.991	.025	.026	-.033	-.015	.007	1.000	.047	.009	-.022	-.098	-.028	.991	.025	.026	-.033	-.015	.007	1.000	.047	.009	-.022	.026	-.033
F10	.162	-.095	.000	.086	.172	-.035	.135	.011	.047	1.000	.549	.101	.162	-.095	.000	.086	.172	-.035	.135	.011	.047	1.000	.549	.101	.172	-.035
F11	.113	-.123	-.024	.078	.069	.100	.007	-.007	.009	.549	1.000	-.004	.113	-.123	-.024	.078	.069	.100	.007	-.007	.009	.549	1.000	-.004	.069	.100
F12	.035	.000	-.027	.023	.033	-.023	.706	-.011	-.022	.101	-.004	1.000	.035	.000	-.027	.023	.033	-.023	.706	-.011	-.022	.101	.104	-.119	-.002	.438
F13	-.123	.000	-.079	1.000	1.000	-.056	.013	.159	.026	.172	.069	.033	.104	-.119	-.002	.438	1.000	-.056	.013	.159	.026	.172	.269	-.009	.002	.331

F14	-.024	-.027	-.069	.047	-.056	1.000	-.013	-.013	-.033	-.035	.100	-.023	.269	-.009	.002	.331	-.056	1.000	-.013	-.013	-.033	-.035	.033	-.006	-.014	.022
F15	.078	.023	.365	.009	.013	-.013	1.000	-.002	-.015	.135	.007	.706	.033	-.006	-.014	.022	.013	-.013	1.000	-.002	-.015	.135	.047	-.025	-.011	.167
F16	.069	.033	.104	-.022	.159	-.013	-.002	1.000	.007	.011	-.007	-.011	.047	-.025	-.011	.167	.159	-.013	-.002	1.000	.007	.011	-.098	-.028	.991	.025
F17	.100	-.023	.269	.026	.026	-.033	-.015	.007	1.000	.047	.009	-.022	-.098	-.028	.991	.025	.026	-.033	-.015	.007	1.000	.047	.162	-.095	.000	.086
F18	.007	.706	.033	-.033	.172	-.035	.135	.011	.047	1.000	.549	.101	.162	-.095	.000	.086	.172	-.035	.135	.011	.047	1.000	.113	-.123	-.024	.078
F19	-.123	.000	-.079	-.015	.069	.100	.007	-.007	.009	.549	1.000	-.004	.113	-.123	-.024	.078	.069	.100	.007	-.007	.009	.549	.104	-.119	-.002	.438
F20	.035	.000	-.027	.023	.033	-.023	.706	-.011	-.022	.101	-.004	1.000	.035	.000	-.027	.023	.033	-.023	.706	-.011	-.022	.101	.104	-.119	-.002	.438
F21	.367	.104	.269	.033	.047	-.098	.162	.113	.035	1.000	-.079	-.069	.365	.104	.269	.033	.047	-.098	.162	.113	.035	.104	.269	-.009	.002	.331
F22	-.095	-.119	-.009	-.006	-.025	-.028	-.095	-.123	.000	-.079	1.000	.006	-.095	-.119	-.009	-.006	-.025	-.028	-.095	-.123	.000	-.119	-.009	-.006	-.014	.022
F23	.032	-.002	.002	-.014	-.011	.991	.000	-.024	-.027	-.069	.006	1.000	.032	-.002	.002	-.014	-.011	.991	.000	-.024	-.027	-.002	.002	-.025	-.011	.167
F24	1.000	.438	.331	.022	.167	.025	.086	.078	.023	.365	-.095	.032	1.000	.438	.331	.022	.167	.025	.086	.078	.023	.438	.331	-.028	.991	.025
F25	.438	1.000	-.056	.013	.159	.026	.172	.069	.033	.104	-.119	-.002	.438	1.000	-.056	.013	.159	.026	.172	.069	.033	1.000	-.056	-.095	.000	.086
F26	.331	-.056	1.000	-.013	-.013	-.033	-.035	.100	-.023	.269	-.009	.002	.331	-.056	1.000	-.013	-.013	-.033	-.035	.100	-.023	-.056	1.000	-.123	-.024	.078

Table 4.18 shows that most of the figures were highly correlated with screening of applicants during recruitment and mitigation strategies which commercial banks in Kenya could use to manage insider information security threats. These include: the use of data encryption at 0.365; Monitoring and responding to suspicious or disruptive behavior of employees 0.367; establishing a formal grievance procedure for staff to vent their feelings at 0.438; setting up an easy and confidential system for staff to report any abnormal behavior from their colleagues at 0.331.

4.6.3 Communalities

Communalities indicate the amount of variance in each variable that is accounted for. Small values indicate variables that do not fit well with the factor solution, and should possibly be dropped from the analysis and once they are dropped what remains will for the factors to be tested and thus the table below.

Table 4.19 Communalities

	Initial	Extraction
Consistently enforcing of policies and controls	1.000	.994
Use of Data Loss Prevention suites (e.g. Restrictions on removal media like flash disks, CDs, etc.)	1.000	.965
Instituting periodic security awareness training for all employees	1.000	.850
Use of data encryption	1.000	.849
Logging and monitoring employee online actions	1.000	.830
Developing an insider incident response plan	1.000	.768
Regular review of information security processes, policies and standards	1.000	.768
Use of Structured defense against remote attacks (e.g. Installation of firewalls)	1.000	.760
Strengthening of Internal controls and monitoring of information system transactions	1.000	.758
Implementing system change controls	1.000	.739
Regular vulnerability assessments	1.000	.739
Implementing secure backup and recovery processes	1.000	.694
Screening of applicants during recruitment	1.000	.685
Use extra caution with system administrators and technical or privileged users	1.000	.658

Deactivating computer access following staff termination	1.000	.564
Anticipation and management of negative workplace issues	1.000	.564
Considering insider threats in the software development life cycle	1.000	.529
Role Based Access Control and/or Dual Access control	1.000	.529
Setting up an easy and confidential system for staff to report any abnormal behavior from their colleagues	1.000	.377
Monitoring and responding to suspicious or disruptive behavior of employees.	1.000	.307
Implementing strict password and account management policies and practices.	1.000	.307
Warning of all staff to be alert to anyone asking for sensitive or restricted information	1.000	.277
Tracking and securing of the physical environment (e.g. use biometric systems)	1.000	.260
Stringent Service Level Agreements with third party service providers	1.000	.260
Enforcement of separation of duties and least privilege	1.000	.246
Establishing a formal grievance procedure for staff to vent their feelings	1.000	.146

Extraction Method: Principal Component Analysis.

Table 4.19 shows the critical mitigation strategies to manage insider information security threats; with the highest rated being consistently enforcing of policies and controls 99.4%; Use of Data Loss Prevention suites (e.g. Restrictions on removal media like flash disks, CDs, etc.) (96.5%); instituting periodic security awareness training for all employees; use of data encryption; Logging and monitoring employee online action; developing an insider incident response plan; Regular review of information security processes, policies and standards at 76.8%. The least adopted mitigation strategies are; stringent Service Level Agreements with third party service providers (26.0%); enforcement of separation of duties and least privilege (24.6%); and establishing a formal grievance procedure for staff to vent their feelings (14.6%).

4.6.4 Total Variance Explained

Table 4.20 Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.068	17.236	17.236	2.068	17.236	17.236	1.999	16.660	16.660
2	1.998	16.653	33.889	1.998	16.653	33.889	1.723	14.357	31.017
3	1.706	14.216	48.105	1.706	14.216	48.105	1.617	13.479	44.496
4	1.399	11.657	59.761	1.399	11.657	59.761	1.588	13.236	57.732
5	1.195	9.960	69.722	1.195	9.960	69.722	1.439	11.990	69.722

Extraction Method: Principal Component Analysis.

Table 4.20 shows that the first five mitigation strategies explain a total of 69.722% of the total variance and this shows their significance in the analysis. Since these five factors have all factors with Eigenvalues greater than 1, they are used in further analysis. Rotation has the effect of optimizing the factor structure and one consequence for these data is that the relative importance of the five factors is equalized. For example factor one before ration accounted for 17.236% of the variance and after rotation it accounted for 16.660% of the variance.

Table 4.21Rotated Component Matrix

	Component				
	1	2	3	4	5
Screening of applicants during recruitment	-.096	.044	.158	**.693**	.108
Consistently enforcing of policies and controls	-.009	.034	-.281	-.015	**.559**
Instituting periodic security awareness training for all employees	**.997**	-.011	-.017	-.007	-.011
Use of data encryption	.059	.025	.033	**.648**	-.255
Use of Structured defense against remote attacks (e.g. Installation of firewalls)	.015	.030	.157	.067	**.796**
Regular vulnerability assessments	.021	-.042	-.049	**.816**	-.191
Stringent Service Level Agreements with third party service providers	-.003	**.912**	.039	.010	-.011
Strengthening of Internal controls and monitoring of information system transactions	-.019	-.016	-.083	-.045	**.606**
Regular review of information security processes, policies and standards	**.996**	-.010	.034	-.050	.021
Implementing strict password and account management policies and practices.	.020	.132	**.859**	.011	.069
Anticipation and management of negative workplace issues	-.011	-.045	**.589**	.109	-.075
Role Based Access Control and/or Dual Access control	-.016	**.921**	.010	.006	.004
Enforcement of separation of duties and least privilege	**.772**	.448	.046	-.019	-.016
Use of Data Loss Prevention suites (e.g. Restrictions on removal media like flash disks, CDs, etc.)	**.827**	-.079	.039	**.996**	-.010
Implementing secure backup and recovery processes	**.722**	-.195	.229	.020	.132
Logging and monitoring employee online actions	**.801**	.081	.129	-.011	-.045
Implementing system change controls	-.128	-.044	**.587**		.044
Tracking and securing of the physical environment (e.g. use biometric systems)	-.042	-.049	**.816**	-.191	.034
Use extra caution with system administrators and technical or privileged users	**.921**	.039	.010	-.011	-.011
Developing an insider incident response plan	-.016	-.083	-.045	**.606**	.025

Monitoring and responding to suspicious or disruptive behavior of employees.	-.010	.034	-.050	.021	.030
Deactivating computer access following staff termination	.132	**.859**	.011	.069	-.042
Considering insider threats in the software development life cycle	-.045	**.789**	.109	-.075	**.921**
Warning of all staff to be alert to anyone asking for sensitive or restricted information	**.921**	.010	.006	.004	-.016
Establishing a formal grievance procedure for staff to vent their feelings	.448	.046	-.019	**.648**	.025
Setting up an easy and confidential system for staff to report any abnormal behavior from their colleagues	**.859**	.109	-.075	-.016	.033

Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization. a Rotation converged in 5 iterations.

Component 1 loads highly with the mitigation strategies; Instituting periodic security awareness training for all employees; regular review of information security processes, policies and standards; enforcement of separation of duties and least privilege; use of Data Loss Prevention suites (e.g. Restrictions on removal media like flash disks, CDs, etc.); implementing secure backup and recovery processes; logging and monitoring employee online actions; use extra caution with system administrators and technical or privileged users; warning of all staff to be alert to anyone asking for sensitive or restricted information; and setting up an easy and confidential system for staff to report any abnormal behavior from their colleagues.

Component 2 loads highly with: Stringent Service Level Agreements with third party service providers; role Based Access Control and/or Dual Access control; deactivating computer access following staff termination; considering insider threats in the software development life cycle.

Table 4.22 Isolation of Factors

Mitigation Strategies Employed	Factor Component
Instituting periodic security awareness training for all employees	**Factor 1**
Enforcement of separation of duties and least privilege	
Regular review of information security processes, policies and standards	
Use of Data Loss Prevention suites (e.g. Restrictions on removal media like flash disks, CDs, etc.)	
Implementing secure backup and recovery processes	
Logging and monitoring employee online actions	
Use extra caution with system administrators and technical or privileged users	
Warning of all staff to be alert to anyone asking for sensitive or restricted information	
Setting up an easy and confidential system for staff to report any abnormal behavior from their colleagues	
Stringent Service Level Agreements with third party service providers	**Factor 2**
Role Based Access Control and/or Dual Access control	
Deactivating computer access following staff termination	
Considering insider threats in the software development life cycle	
Implementing strict password and account management policies and practices	**Factor 3**
Anticipation and management of negative workplace issues	
Implementing system change controls	
Tracking and securing of the physical environment (e.g. Use biometric systems)	
Screening of applicants during recruitment	**Factor 4**
Use of data encryption	
Regular vulnerability assessments	
Use of Data Loss Prevention suites (e.g. Restrictions on removal media like flash disks, CDs, etc.)	
Developing an insider incident response plan	
Establishing a formal grievance procedure for staff to vent their feelings	
Consistently enforcing of policies and controls	**Factor 5**
Use of Structured defense against remote attacks (e.g. Installation of firewalls)	
Strengthening of Internal controls and monitoring of information system transactions	

The study extraction gave out 5 components. Component one was composed of; instituting periodic security awareness training for all employees, enforcement of separation of duties and least privilege, regular review of information security processes, policies and standards, use of Data Loss Prevention suites (e.g. Restrictions on removal media like flash disks, CDs, etc.), implementing secure backup and recovery processes, logging and monitoring employee online actions, use extra caution with system administrators and technical or privileged users, warning of all staff to be alert to anyone asking for sensitive or restricted information, and setting up an easy and confidential system for staff to report any abnormal behavior from their colleagues.

Component 2 comprised of stringent service level agreements with third party service providers, role based access control and/or dual access control, deactivating computer access following staff termination, considering insider threats in the software development life cycle.

Component 3 comprised of; implementing strict password and account management policies and practices, anticipation and management of negative workplace issues, implementing system change controls, tracking and securing of the physical environment (e.g. Use biometric systems), screening of applicants during recruitment.

Component 4 comprised of; screening of applicants during recruitment, use of data encryption, Regular vulnerability assessments, use of data loss prevention suites (e.g. restrictions on removal media like flash disks, CDs, etc.), developing an insider incident response plan, establishing a formal grievance procedure for staff to vent their feelings.

Component 5 comprised ofconsistently enforcing of policies and controls, use of structured defense against remote attacks (e.g. Installation of firewalls), strengthening of internal controls and monitoring of information system transactions.

Table 4.22 highlights the categories of the various mitigating strategies and the impact levels once applied. Banks should continuously and to a great extent utilize the mitigating strategies highlighted in Factors 5 and 4.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

The objectives of this study were; to determine the nature of Insider Threats facing Commercial Banks in Kenya and to determine mitigation strategies which commercial banks could use to manage insider information threats. This research study was conducted on the commercial banks and the response rate achieved was 72%. Though the entire population of 43 banks was targeted, 31respondentsdid fill the questionnaire.

5.2 Summary

It may be concluded, at least in the banking industry, that the field of information security professionals is male dominated. This was discovered from the respondents' gender, in that they were all male. The pure insider is undoubtedly the greatest concern to commercial banks in Kenya. This is according to 93% of the respondents in the study. Attacks from within the organization are now a greater challenge and now present a larger threat because pure insiders have all the access and therefore the capacity of inflicting the greatest damages by capitalizing on vulnerabilities (Baker, et al., 2008).

Since most of these mitigation strategies are utilized in many of the banks in various degrees, there is need for them to be fortified. This could be achieved through; training, motivation, creating awareness, and managing of time and workload pressures (Whitman, 2004). Financial gain as a motivation is closely followed by disgruntlement, which was cited to various extents, by 89% of the respondents. These are frustrated employees who may think of harming the organization as a result of their frustration. This therefore means that with an increasing number of frustrated employees also becomes the potential for insider attacks. A key challenge for the banks is the associated cost of information security tools and mitigation strategies.

5.3 Conclusion

Financial gain is highlighted as the single most prevalent motivation for insider threats inbank's experience. In that case, it is considered an economic crime and Kenya is in fact in the lists of the countries that have reported an increase in these kinds of crimes in the past 3 years according to global surveys (GECS, 2011).

The most prevalent type of insider threats in commercial banks was pure insiders. Staffs within the organization have the rightful access to information which they use for their benefits. This finding creates a clear picture to commercial banks that the threat from within is more and requires to be addressed if insider threat was to be effectively controlled. Banks must therefore have paradigm shifts as far as the insider issue is involved. Rather than the traditional approach of sophisticated equipment and complex software solutions, the insider issue must now be seen as a people problem (Rudolph, et al., 2002).

The research reports show that all the banks make considerable efforts as far as mitigations are concerned. The critical mitigation strategies to manage insider information security threats werenotably, strengthening of internal controls and monitoring of information system transactions, regular review of the information security processes, policies and standards, strict password account management policies,use of data loss prevention suites (for example restrictions on removal media like flash disks, CDs, etc.); instituting periodic security awareness training for all employees; use of data encryption; Logging and monitoring employee online action; developing an insider incident response plan; Regular review of information security processes, policies and standards.

5.4 Limitations of the Study

Banks being institutions where confidentiality is crucial to the business do not share risks and threats by insiders to outsiders in fear of reputational risk consequences. Competition within the banks also ensures insider details are not released to the public, hence limited or minimal information could be released.

Human factors and insider behavior are not easy to analyze, lack of consistency in the behavioral patterns has impact in getting the correct trends in characteristics and motives of the insiders.Human behaviors is not easy to track and thus insider threats which have been committed and professionally concealed by destroying the trace records substantially affects the study since the true picture of the extend of insider threats is not revealed.

In the course of the study, time was a limiting factor. In some cases it was difficult to get sufficient time to go through the questionnaires with the respondents, other times the respondents could not have focused attention and likewise due to the qualitative nature of the study, more time in the study could have been appropriate.

Most of the banks owned or with majority foreign ownership shares havetheir data stored and managed outside the country hence the local teams do not have full knowledge of the controls in place.

Many banks are still in denial of the fact that insider threats poses a big challenge, acceptance of the fact that those in trusted positions may cause the greatest harm to the institution is lacking in most banks.

5.5 Recommendation for further Research

In response to increasing recognition of the dangers posed by insider threat to information systems, a study to improve the understanding of the personality, motives and circumstances which contribute to information technology insider actions will be of benefit to banks and other financial institutions.The goal of the study is to contribute to improvements in security, law enforcement and counter intelligence policies and practices. Specific solutions e.g. applications for improving screening, selection, monitoring and management of information technology specialists are the primary goals of the research.

The effects of technology advancement and workers demanding "technology democracy", that is freedom to use IT applications and devices of their choice in order to communicate and conduct their work more effectively and upcoming technologies namely cloud, mobile, social and outsourcing are likely to increase the avenues of insider threats. A research to study how commercial banks could manage the access and prevent insider threat activities is required. Techno savvy staff can exploit opportunities arising from the system knowledge to cause more harm to the banks.

The challenges encountered by banks in implementing the insider threat mitigating strategies are of concern as per the findings of this study. A research on the challenges and how banks can overcome them will be a big contributor in ensuring the current gaps are sealed.

REFERENCES

AeranAnkur, "Comprehensive overview of INSIDER THREATS and their controls", 2006.***www.cccure.org/Documents./InsiderThreatsReport.pdf***

Anderson Bill, "Insider threat: the game has changed", June 14th 2012. S.C. Magazine.http://www.scmagazine.com/insider-threat-the-game-has-changed/article/245759/ . [Accessed 19th June, 2012].

Bace, R.G. (2002). Vulnerability assessment and intrusion detection systems.In S.

Bosworth and M. E. Kabay (Eds.), Computer Security Handbook, 4th ed. New York: John Wiley and Sons, Inc.

Baker, W.H., Hylender, C.D. and Valentine, J.A. (2008).*2008 Data Breach Investigations Report*.http://www.verizonbusiness.com/resources/security/databreachreport.pdf. Accessed: June 13, 2012

Barman, S. (2002). Writing Information Security Policies. Indianapolis: New Riders.

Brown S., Uncloaking the Insider Threat, "Uncloaking the Insider Threat", May 2002. http://security.ittoolbox.com/pub/SB052002.pdf

Brussin, D. (2002). Firewall and proxy servers. In S. Bosworth and M. E. Kabay (Eds.), Computer Security Handbook, 4th ed. New York: John Wiley and Sons, Inc.

Bulgurcu, B, Cavusoglu, H. and Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523-548.

CapelliDawn , "Insider Threats: Emerging Risks", Bank Info Security, May 2012. http://www.bankinfosecurity.com/insider-threat-emerging-risks-a-4719 [Accessed June 18, 2012]

CERT, (2009).Common Sense Guide to Prevention and Detection of Insider Threats 3rd Edition – Version 3.1.www.cert.org/archive/pdf/CSG-V3.pdf [Accessed June 12, 2012]

Chokhani, S. (2002).Public Key Infrastructures and Certificate Authorities.In S. Bosworth and M. E. Kabay (Eds.), Computer Security Handbook.

Christian W. Probst, Jeffery Hunker, DietarGollman, Matt Bishop, "Insider threats in Cyber Security", (2010).

Cole E. and Ring S., Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft, Syngress Publishing, 2006

Cohen, L. and Felson, M. (1979), "Social change and crime rate trends: A routine activity approach", American Sociological Review, vol. 44, pp. 588–608.

Cole Eric, 2010 " Different Flavors of the Insider Threat". http://www.darkreading.com/blog/227700748/different-flavors-of-the-insider-threat.html [Accessed July 4, 2012]

D'Arcy, J., Hovav, A., and Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research, 20(1), 79-98.

Einwechter N., Preventing and Detecting Insider Attacks Using IDS, 20th March 2002. http://www.securityfocus.com/infocus/1558

EIU. Economist intelligence Unit: Power to the people? Managing technology democracy in the workplace, http://graphics.eiu.com/marketing/pdf/Technology%20Democracy.pdf; June 2009.

International Organisation for Standardisation, ISO/IEC 17799:2000(E) Information technology – Code of practice for information security management, 1st Edition December 2000

Flinders K, "Employees will choose their own computers in 2010", Computer Weekly January 2010.Computer Weekly, http://www.computerweekly.com/ Articles/2010/01/19/239999/Employees-will-choose-theirown-Computers-in-2010.htm;2010.

Grace Duffield and Peter Grabosky - The Psychology of Fraud, No. 199, March 2001. ISSN 0817–8542, ISBN 0 642 24224 0.

GECS (Global Economic Crime Survey), 2011 By Price Waterhouse Coopers. www.pwc.com/crimesurvey [Accessed on June 12, 2012]

Greitzer, F.L. et al. (2008). Combating the Insider Cyber Threat, *IEEE Security and Privacy 6 (1)*, pp. 61-64.

Hall James, "The Role of Technology in Banking", March 2012. http://importanceoftechnology.net/124/role-of-technology-in-banking [Accessed July 12, 2012]

Haugen, S. and Selin, J.R. (1999). Identifying and controlling computer crime and employee fraud. Industrial Management and Data Systems, 99(8), 340-344.

Hirschi, T. (1969).Causes of Delinquency. Berkeley: University of California Press.

Hollinger, R.C. (1986). Acts against the workplace: Social bonding and employee deviance. Deviant Behavior, 7, 53-75.

James H. L. (1996), Managing Information systems security: a soft approach. Proceedings of the Information Systems Conference of New Zealand. IEEE Society press [http://www.tawileh.net/anas//files/downloads/papers/InfoSec-SME-ISSE.pdf?download] Accessed 12th May, 2010.

Jan Killmeyer, (2006)"Information Security Architecture – An Integrated approach to security in the organization", Second Edition. PP 17.Auerbach Publications, NY.

Kenneth C. Brancik, Inside Computer Fraud. An In-depth Framework for Detecting and Defending Against Insider I.T. Attacks (2008)

Kabay, M.E. (2002). Developing security policies. In S. Bosworth and M. E. Kabay (Eds.), Computer Security Handbook, 4th ed. New York: John Wiley and Sons, Inc.

KantankjiSamer Dr., (2008) "Long-term Challenges and Risks in the Banking Industry".http://www.kantakji.com/fiqh/Files/Banks/90021.pdf [Accessed: July 16, 2012].

KBA (Kenya Bankers Association) 2012, http://www.kba.co.ke/index.php?option=com_contentand

view=articleandid=129:working-together-to-make-banking-betterand_catid=57:slideshow . Accessed July 16, 2012.

Keeney M., E. Kowalski, D. Cappelli, A. Moore, T, Shimeall, S. Rodgers, "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors", Jan 2005.www.cert.org/archive/pdf/insidercross051105.pdf [Accessed July 12, 2012]

Kenya Bankers Association, "A Report on the Trends of Fraud", 2010, pp 2-12 [Available from the association upon official request]

Kioko Sammy, "Banking Fraud worry payment security Experts". December 14, 2011.http://www.businessdailyafrica.com/Corporate+News/-/539550/1289190/-/s9v0yg/-/index.html. Accessed: June 15, 2012.

Marisa Reddy Randazzo, Ph.D. Dawn Cappelli Michelle Keeney, Ph.D. Andrew Moore Eileen Kowalski, "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector",2004 www.cert.org/archive/pdf/bankfin040820.pdf

Merrit Maxim, "Defending against Insider threats to reduce your I.T. Risk", March 2012. White paper, Accessed 20th June 2012. http://www.ca.com/~/media/Files/whitepapers/insider-threat-wp-jan-2011.pdf

Mukinda Fred, "Sh 500 Million lost to Kenya Bank Fraud in just a month", January 13, 2011. Daily Nation, http://www.nation.co.ke/News/Sh500m%20lost%20to%20bank%20fraud%20in%20just%20a%20month%20/-/1056/1089298/-/s98rt1/-/index.html .Accessed: July 16, 2012.

PWC (PricewaterhouseCoopers) 2011, "A step ahead: Economic Crime in Kenya", November 2011. www.pwc.com/ke . Accessed: July 16, 2012.

Ravich George, "Security and Fraud are Top Issues Facing Banking Industry", August 2011. http://www.fx-mm.com/7490/news/security-and-fraud-prevention-are-top-issues-facing-banking-industry/ [Accessed: July 13, 2012]

Research Foundation, Threats to Computer Systems, 14 August 2006,http://rf-web.tamu.edu/security/secguide/V1comput/Threats.htm

Rudolph, K., Warshawsky, G. and Numkin, L. (2002).Security Awareness. In S. Bosworth and M. E. Kabay (Eds.), Computer Security Handbook, 4th ed. New York: John Wiley and Sons, Inc.

Sandhu, R. (2002). Identification and Authentication. In S. Bosworth and M. E. Kabay (Eds.), Computer Security Handbook, 4th ed. New York: John Wiley and Sons, Inc.

Schultz Eugene, "Predicting, Detecting and Responding to Insider Attacks" December 2008. Network Security Consulting Blog, http://blog.emagined.com/2008/12/01/predicting-detecting-and-responding-to-insider-attacks/ [Accessed: July 14, 2012]

Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers and Security 21 (6), pp 526-531*

Schultz E. E. and R. Shumway, Incident response: A strategic guide for system and network security breaches. (Indianapolis: New Riders, 2001) p. 189.

Shaw Eric, Ph.D., Keven G. Ruby, M.A. and Jerrold M. Post, M.D. *"The Insider Threat to Information Systems - The Psychology of the Dangerous Insider"* Security Awareness Bulletin No. 2 – 98, 2005.http://home.engineering.iastate.edu/~guan/course/CprE-536/paperreadinglist606/profiling/sab.pdf [Accessed: June 14, 2012].

Standard Digital (January 25, 2012). "*We are paying too much for cybercrime"*http://www.standardmedia.co.ke/?id=2000050341and cid=17and story=WeandarticleID=2000050341

Stanton, M.S., Stam, K.R., Guzman, I. and Caldera, C. (2003).Examining the linkage between organizational commitment and information security. Paper presented at the Proceedings of the IEEE Systems, Man, and Cybernetics Conference, Washington, DC.

T. Tuglularand E.H. Spafford, "A framework for characterization of insider computer misuse," unpublished paper, (Purdue University, 1997).

US Secret Service and CERT Coordination Centre, Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector, August 2004,http://www.cert.org/archive/pdf/bankfin040820.pdf

United Press International, '*Computer Criminals Have Big Pay Days',* April 5, 1981.ThePittsburgh Press.http://news.google.com/newspapers?nid=1144and dat=19810405and id=yGgdAAAAIBAJandsjid=JV0EAAAAIBAJand pg=4048,1549010 Accessed: 13th July, 2012.

W. KragBrotby, CISM, Senior Security Consultant, USA, *"Information Security GovernanceGuidance for Information Security Managers*") ISBN 978-1-933284-73-6 [2008].

W.E.F([World Economic Forum) 2011 Report.http://reports.weforum.org/wp-content/blogs.dir/1/mp/uploads/pages/files/global-risks-2011.pdf [Accessed: June 15, 2012]

Whitman, M.E. (2004). In defense of the realm: Understanding the threats to information security. International Journal of Information Management, 24, 43-57.

APPENDIXIES

APPENDIX ONE

RE: LETTER OF INTRODUCTION

I am DOMINIC K. MULWA, undertaking Masters of Business Administration course at the University of Nairobi.

I am undertaking research on insider information security threats among commercial banks in Kenya, leading to the production of my master's project report.

I would be grateful if you would volunteer to assist in this project, by consenting to completing a questionnaire which covers certain aspects of the topic.

Be assured that any information provided will be treated in the strictest confidence and none of the participants will be individually identifiable in the resulting report.

Thanks in advance for supporting my efforts in achieving the course expectations.

Best Regards,

Mulwa D. K.

_____ _____

Supervisor: Chairman, Department of Management Information Sciences

APPENDIX TWO

Research Questionnaire

I am undertaking a research on insider information security threats among commercial banks in Kenya as part of my academic qualifying requirement. Your assistance, through completion of this questionnaire will be highly appreciated.

Any information provided will be treated in confidence.

Thank you in advance for taking time to fill in the questionnaire.

SECTION A: DEMOGRAPHIC INFORMATION

1. Please tick to indicate your Gender

   Male …… ( )

   Female……. ( )

2. Please tick the age bracket in years in which your age falls

   Below 25……. ( )
   Between 25 and 30……. ( )
   Between 31 and 35……. ( )
   Between 36 and 40……. ( )
   Between 41 and 45……. ( )
   46 and above…… ( )

3. Please indicate your Position/Designation in the bank

   IT Manager…… ( )
   Chief Information Officer (CIO)…….. ( )
   Chief Information Security Officer (CISO)……. ( )
   IT consultant……. ( )
   Chief Executive Officer …… ( )

   Others [*Specify*] …….

4. For how long have you worked in your current position in the bank?

   Below 5 years…….. ( )

   Between 6 and 10 years……. ( )
   Between 11 and 15 years…… ( )
   Between 16 and 20 years…… ( )
   Between Over 20 years…… ( )

5. For how long has your bank been in operation?

   Below 5 years…….( )
   Between 6 and 10 years…….. ( )
   Between 11 and 15 years…… ( )
   Between 16 and 20 years…… ( )
   Over 20 years ……. ( )

6. What is the current shareholding structure of your bank?

   Locally owned institution…… ( )

   Government controlled majority shares institution……. ( )

   Foreign owned but locally incorporated…….. ( )

   Foreign owned NOT locally incorporated…… ( )

   Owned by both local and foreigners…… ( )

   Other [*Specify*]……
   …….

   …….

7. What is the size of the bank in terms of total assets value in Kenya Shillings?

   Below 5 billion ……. ( )

   Between 5 and 20 billion…….. ( )

   Between 20 and 50 billion…… ( )

   Between 50 and 100 billion……( )

   Between 100 and 200 billion……..( )

   Above 200 billion……( )

8. Please tick to indicate the number of employees in your bank

   Below 100…….. ( )

   Between 101 and 500…… ( )

   Between 501 and 1000……... ( )

   Between 1001 and 5000……. ( )

   Above 5000…….. ( )

9. Please tick to indicate the number of branches owned by the bank in Kenya.

   Below 10 ……. ( )

   Between 11 and 30…… ( )

   Between 31 and 50……. ( )

   Between 51 and 70…….. ( )

   Between 71 and 100…… ( )

   Above 100…….. ( )

SECTION B: TYPES OF INSIDER THREATS

10. Please tick to indicate the extent to which your bank has encountered each of the following insider threats.

Insider Threats	**No Extent at All**	**Little Extent**	**Moderate Extent**	**Great Extent**	**Very Great Extent**
Sabotage (disrupting operations)					
Theft (stealing information)					
Spoofing(pretending to be something or someone that one is not)					
Viruses					
Social engineering (manipulation of users to obtain information)					
Installation of unauthorized software					
Hacking(accesses a computer system by circumventing its security system)					
Purposefully installing malicious software					
Impersonation of other users					
Physical security breaches					
Tampering with data (unauthorized changes of data or records)					
Unauthorized Access					
Destruction of critical data					

Denial of service attacks					
Organized Crime(Insiders colluding with criminal gangs)					
Identity Thieves(Impersonation Fraudsters)					
Activists(to bring social or political change through actions)					
Password Cracking					
Phishing (acquiring information and/or money from people without their knowledge)					
Key loggers(hardware or software-based, they capture keystrokes)					
Selling employer's confidential information to the competitor(s)					
Others *[Specify and Rate accordingly]*					

11. Please tick to indicate the extent to which perpetrators of insider threats in your bank have or have exhibited/displayed the following characteristics.

Characteristics	**No Extent at All**	**Little Extent**	**Moderate Extent**	**Great Extent**	**Very Great Extent**
Have Criminal tendencies					
Have a reduced sense of loyalty					
Social transgression tendencies					
High ethical flexibility					

Emotional distress					
Resistance to authority					
Lack of empathy (disregard for the impact of other peoples actions)					
Introversion(often loners)					
Mostly depressed					
Frustration with the workplace					
Across system usage patterns(Unusual system usage patterns)					
Making of Meaningful errors					
Deliberate markers (leave small, intentional signs)					
Weakness in handling conflicts					
Curiosity to learn systems both operations and technical					
Have Tendencies to work extended hours and preferably late nights and weekends					
Obsessive tendencies (continuously pre-occupied)					
Imitation and modeling those whom they respect					
Others *[Specify and Rate accordingly]*					

12. Please tick to indicate the extent to which each of the following types of insiders has perpetrated insider threats/attacks in your bank.

Types of Insiders	**No Extent at All**	**Little Extent**	**Moderate Extent**	**Great Extent**	**Very Great Extent**
Pure Insider [*employee with all rights and access*]					
Insider associate [*guards, cleaners, contractors, service providers*]					
Insider affiliate [*friend, spouse, client who uses employee credentials*]					
Outside affiliate [*outsiders who use open access and vulnerabilities*]					
Others *[Specify and Rate accordingly]*					

13. What is the average age in years of the perpetrators of insider threats encountered in your bank?

Below 25…….. ( )
Between 25 and 30…… ( )
Between 31 and 35…… ( )
Between 36 and 40…… ( )
Between 41 and 45……..( )
46 and above…… ( )

14. Please tick to indicate the extent to which the following motivations could have been the driving force behind the insider threats experienced in your bank.

Motivation	**No Extent at All**	**Little Extent**	**Moderate Extent**	**Great Extent**	**Very Great Extent**
Financial gain–(stealing or manipulating financial details for personal monetary benefits)					
Disgruntlement (Frustrated employee will think of harming the company).					
Espionage (spy or mole that is influenced by criminals or competitors targeting the bank)					
Quest for challenge (explore the world around or take it as a challenge)					
Revenge (employees with negative feelings towards the company or individuals within the company)					
Desire for respect(Employees desiring to proof themselves because they are less skilled than others)					
Emotional distress(Employee is highly frustrated)					

Sabotage (disruption of company operations)					
Theft (data stored in computer hardware and software, company or customer financial data)					
Curiosity (experimenting with company'snetwork resulting in disruption of services)					
Hooliganism(such as defacing a Web site)					
General malice					
Politics (internally or externally instigated)					
Challenge security professionals					
Others *[Specify and Rate accordingly]*					

SECTION C: MITIGATION

15. To what extent has the bank employed the following strategies for mitigating Insider attacks?

Mitigation Strategies	**No Extent at All**	**Little Extent**	**Moderate Extent**	**Great Extent**	**Very Great Extent**
Screening of applicants during recruitment					
Consistently enforcing of policies and controls					
Instituting periodic security awareness training for all employees					
Use of data encryption					
Use of Structured defense against remote attacks (e.g. Installation of firewalls)					
Regular vulnerability assessments					
Stringent Service Level Agreements with third party service providers					
Strengthening of Internal controls and monitoring of information system transactions					
Regular review of information security processes, policies and					

standards					
Implementing strict password and account management policies and practices.					
Anticipation and management of negative workplace issues					
Role Based Access Control and/or Dual Access control					
Enforcement of separation of duties and least privilege					
Use of Data Loss Prevention suites (e.g. Restrictions on removal media like flash disks, CDs, etc.)					
Implementing secure backup and recovery processes					
Logging and monitoring employee online actions					
Implementing system change controls					
Tracking and securing of the physical environment (e.g. use biometric systems)					
Use extra caution with system administrators and technical or privileged users					
Developing an insider incidentresponse plan					

Monitoring and responding to suspicious or disruptive behavior of employees.					
Deactivating computer access following staff termination					
Considering insider threats in the software development life cycle					
Warning of all staff to be alert to anyone asking for sensitive or restricted information					
Establishing a formal grievance procedure for staff to vent their feelings					
Setting up an easy and confidential system for staff to report any abnormal behavior from their colleagues					
Others [Specify and Rate accordingly]					

16. Please tick to indicate to what extent has the bank has experienced each of the following challenges in implementation of insider threats mitigation strategies.

Challenges	**No Extent at All**	**Little Extent**	**Mode rate Extent**	**Great Extent**	**Very Great Extent**
High costs of acquiring, licensing and maintaining the security solutions.					
Lack of technical experience in using security tools					
Lack of knowledge on the banks policies on information use					
Difficulty in achieving clear staff background screening					
Lack of staff security training					
Vendor/Contractor management Issues					
Poor Communication flow within the organization					
Insufficient Audit trails					
Technology advancement increasing opportunities for insiders					
Complexity of the security tools					
Job stress due to workload pressure					
Others *[Specify and Rate accordingly]*					

APPENDIX THREE

List of Commercial Banks in Kenya

1. African Banking Corporation Ltd.
2. Bank of Africa Kenya Ltd.
3. Bank of Baroda (K) Ltd.
4. Bank of India
5. Barclays Bank of Kenya Ltd.
6. CFC Stanbic Bank Ltd.
7. Charterhouse Bank Ltd
8. Chase Bank (K) Ltd.
9. Citibank N.A Kenya
10. Commercial Bank of Africa Ltd.
11. Consolidated Bank of Kenya Ltd.
12. Co-operative Bank of Kenya Ltd.
13. Credit Bank Ltd.
14. Development Bank of Kenya Ltd.
15. Diamond Trust Bank (K) Ltd.
16. Dubai Bank Kenya Ltd.
17. Eco bank Kenya Ltd
18. Equatorial Commercial Bank Ltd.
19. Equity Bank Ltd.
20. Family Bank Ltd
21. Fidelity Commercial Bank Ltd
22. Fina Bank Ltd
23. First community Bank Limited
24. Giro Commercial Bank Ltd.
25. Guardian Bank Ltd
26. Gulf African Bank Limited
27. Habib Bank A.G Zurich
28. Habib Bank Ltd.
29. Imperial Bank Ltd
30. I and M Bank Ltd
31. Jamii Bora Bank Ltd.
32. Kenya Commercial Bank Ltd
33. K-Rep Bank Ltd
34. Middle East Bank (K) Ltd
35. National Bank of Kenya Ltd
36. NIC Bank Ltd
37. Oriental Commercial Bank Ltd
38. Paramount Universal Bank Ltd
39. Prime Bank Ltd
40. Standard Chartered Bank (K) Ltd
41. Trans-National Bank Ltd
42. Victoria Commercial Bank Ltd
43. UBA Kenya Bank Ltd.