ADDIS ABABA UNIVERSITY
SCHOOL OF GRADUATE STUDIES

SCHOOL OF INFORMATION SCIENCE

(EXTENSION PROGRAMME)

Assessment of Insider Threat in Ethiopian Banking Industry

A Thesis Submitted to the School of Graduate Studies of Addis Ababa University in Partial Fulfillment of the Requirements for the Degree of Master of Science in Information Science

By:
Behabtu Amare

Advisor:
Workshet Lamenew (Phd)

JUNE, 2015

ADDIS ABABA UNIVERSITY SCHOOL

OF GRADUATE STUDIES SCHOOL OF

INFORMATION SCIENCE

(EXTENSION PROGRAMME)

Assessment of Insider Threat In Ethiopian Banking Industry

By:

BEHABTU AMARE

Name and Signature of Members of the Examining Board

Name	**Title**	**Signature**	**Date**
_____	Chairperson,	_____	_____
_____	Advisor,	_____	_____
_____	Examiner,	_____	_____

DEDICATION

I would like to dedicate this paper to my GOD, who allows me to start and come to the end, and always supports to pass all the challenges I went through.

Thank you

ACKNOWLEDGEMENT

First and foremost, I would like to give my sincere appreciation to my mother and my father; they have been foremost in my thoughts throughout my endeavors. I am truly blessed to have them in my life. Their understanding in regards to the time required away from them to complete this endeavor and their positive attitudes and occasional hugs have made it easier to cope with my feelings of being overwhelmed.

I would like to thank my advisor, Dr. Workshet Lamenew. His help in pointing me to the right direction in my research and his advices on the unexpected bumps in the road were instrumental in my completing this thesis. His attitude and enthusiasm allowed me to welcome the challenge and overcome obstacles.

Special thanks must also go to my family, My brothers Gebra Amarea and Mulugeta Amare, my sister Aberash Amare ,W/o Fikrte Atelabachew and Ato Asefa Aurga ,for their understanding and love. You are the motivating force behind me at all times through both the highs and lows of my time in graduate school. Thank you for everything you give me.

Table of Contents

CHAPTER THREE

CHAPTER FOUR

CHAPTER FIVE

List of Table

List of Figures

List of Acronyms and Abbreviation

CBE	Commercial Bank of Ethiopia
CERT	Computer Emergency Response Team (Carnegie Mellon University)
CMU	Carnegie Mellon University
CSI	Computer Security Institute
GECS	Global Economic Crime Survey
RBAC	Role-Based Access Control
NBE	National Bank of Ethiopia
ICT	Information and Communications Technology
IEC	International Electro technical Commission
INSA	Intelligence and National Security Alliance
IP	Intellectual Property
NIST	National Institute of Standards and Technology
ISO	International Organization for Standardization
IT	Information Technology
ITSRA	Insider Threat Security Reference Architecture
SDLC	System Development Life Cycle
SEI	Software Engineering Institute
HR	Human Resource
SIEM	Security Information and Event Management
SPSS	Statistical Package for the Social Science
VPN	Virtual Private Network

ABSTRACT

This thesis work examines the insider threat management of Ethiopian banking industry with particular emphasis on the insider threat, the motivational factors that leads insider to commit malicious activities and try to see the current implemented insider threat mitigation strategies and activities within the commercial banking industry of Ethiopia .In addition to this, those challenges that faces the Ethiopian banking industry in fighting insider also assessed.

This research work made use of the survey research design in its methodology. 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 nineteen commercial banks operating in Ethiopia. Using SPSS Statistical methods such as mean, percentile and correlation were utilized to analyze the data collected from the respondents.

Based on this study, insider threat like the Installation of unauthorized software threat and financial frauds are the some of the prevailed malicious activities of insiders within the Ethiopian banking industry. Most of the mitigation strategies which are mentioned on this study are utilized in many of the banks in various degrees. Dissatisfaction with immediate reporting manager, steal data for monetary gain, desire for recognition, and emotional distress (Employee is highly frustrated) are seems to be a motivation for insider threats.

After identifying those prevailed insider threat and ,motivations within the Ethiopian banking industry ,this study provide recommendation and best practices from different literature review to mitigate those insiders malicious activities within the Ethiopian banking sectors

CHAPTER ONE

1. INTRODUCTION

1.1 Background

Ethiopia is a low income country with a population of 92 million people (World Bank).The banking sector in Ethiopia is one of the rapidly growing sectors of the country's economy (Abiy W. and Lemma L.,2012). For Ethiopia's banking sector, the digital age was slow to come, but it's now taking the industry by storm, as banks, both public and private, are scrambling to make use of the latest banking technologies. Like many other countries around the globe, Ethiopia has embraced ICTs and ICT based services as key enabler for social and economic development in the country (Halefom H., 2014). In the digital information age which we now live in, organizations are seeking to use automation by way of Information Technology to process information in order to better serve their customers.

Some persons have different motivations that are not in keeping with the use of Information Technology within the confines of proper ethical and sometimes even legal conduct (Dwight A., 2012). Unfortunately, not everyone wants to use this advancement for the greater good. Even though the use of IT offers so many advantages to organizations, there are numerous inherent risks that must be mitigated in order to successfully Secure Ethiopian banking sector services. Based on a recent survey, employee fraud in the financial services industry is a widespread problem that is largely attributed to advances in technology. Employees who have access to these information systems are often the ones with the tendency to steal (Esola, L., 2007).

To enhance the role played by the banks two major policy directions are enshrined (Zerayehu S.et al, 2013). The first direction is to create information system, which will provide full, timely and reliable information with respect to income and properties of borrowers and make the information accessible. As Lemma and Abiy (2012) stated information security awareness in the banking sector in Ethiopia is unsatisfactory. Consequently, the level of proper information security governance in the banking sector in Ethiopia is a critical area of improvement'.

The information security world has recently started becoming aware of another threat that had more devastating consequences and was substantially more difficult to tackle. This time, the threat was not coming only from external hackers, but from authorized users of IT systems. These users abuse their privileged access rights by committing a series of unintentional or deliberate actions damaging individuals or organizations in many different ways. The global information security survey by PwC (2014) reported that the number of security incidents increased 25% in 2013, among which 58% were believed to be performed by current (31%) or former employees (27%). Consistently, Verizon (2013) found an increase of more than 10% of reports regarding security breaches committed by insiders.

The growing threat of the malicious insider has given rise to a number of long term research projects on different sectors of the country. The Information Network Security Agency (INSA) identified several critical infrastructure sectors that require special attention in protecting the cyber space from any possible attacks. Some of them as follow:

- Banking and finance
- Information and telecommunications
- Energy
- Defense base and related technological infrastructures

Information Assets are under serious threats and attacks from insiders day in and out in the government and private Banks. With the advancement of information Communication technology (ICT), Banks collect a lot of confidential information about their, customers, employees and financial status. A lot of the information being collected are processed and stored electronically and with the widespread use of the information technology, the risks of theft and attack are expanding by the day whilst pressure is also being mounted on information security infrastructure. In case any confidential information such as customer's information and trade secrets fall into wrong hands, it will lead to negative consequences like loss of goodwill, customers and profit. In a financial institution such as a bank, likely targets are customer account records or perhaps company accounts, where there is a direct access to funds.

Information security in finance and banking can be increased by striving certain objectives like availability, integrity, confidentiality .All banks and their branches in the Ethiopian

Banking Industry will need to balance between giving employees real-time access to applications and information, and addressing the corresponding concern for the security of information assets and the information systems. Balancing these needs necessitates secure information systems. The availability, integrity, confidentiality (CIA) Triad is a venerable, well-known model for security policy development, used to identify problem areas and necessary solutions for information security (Terry C.,2013).Specifically, the Bank should be able to ensure the following characteristics of Information .it were a well-known model for information security.

Confidentiality: protecting against unauthorized disclosure and ensuring the authenticity of the data's source. The property that information is not made available or disclosed to unauthorized individuals, entities, or processes

Integrity: preventing unauthorized modification or the property of safe guarding the accuracy and completeness of assets.

Availability: preventing against data delays and denials (removals) and ensuring accessibility to those authorized to do so.

Some of the risks posed from insider threats in the financial sector includes undesired disclosure of confidential customer and account data jeopardizing an organizations most valuable relationship, fraud, loss of intellectual property, disruption to critical infrastructure, Monetary loss and Destabilize, disrupt and destroy cyber assets of financial institutions

In this study the researcher break down the various attributes of the insider threat in Ethiopian banking industry. Finally, the thesis derives recommendations to enhance the current methods to reduce the vulnerability, as well as proposes additional measures to further reduce the threat from banking insiders.

Information Security Management (ISM) is the process of protecting electronic and non-electronic information assets against the risks of loss, misuse, damage, and disclosure or corruption (ISO2001-2:2005).According to Fredrik J. B., (2005), "Information Security Management is the management of information security in organizations". Hence, the concept denotes those activities in the bank related to the direction and control of the security over information assets. Activities include (e.g.) assessment of insider threats and the current state of information security in the bank, design and implementation of administrative (information

security rules for employees, etc.) and technical (access control systems, etc.) security controls, and operation of the day-to-day efforts to preserve information security (documentation of and response to incidents, training of employees, etc

1.2 A Brief History of Banking in Ethiopia

Modern banking in Ethiopia began in Ethiopia in 1905, when the bank of Abyssinia was first established in Addis Ababa under a 50 years franchise agreement with the British owned national bank of Egypt (Belay, 1987). Modern banking increasingly relies on the internet and computer technologies to operate their businesses and market interactions, the threats and security breaches are highly increase in recent years. Insider and outsider attacks have caused global businesses lost trillions of Dollars a year. Private commercial banks become the picture of the Ethiopian economy after the historical proclamation of licensing and Supervision of Banking Business Proclamation No.84/1994 of Ethiopia to undertake commercial banking activities. This proclamation is the foundation of private banking in Ethiopia after the revolution. Despite the prevailing improvement in branch expansion, Ethiopia remains one of the under-banked economies even at sub-Saharan African countries standard (Teklebirhan, 2008).

Ethiopian banking system is one of the most underdeveloped compared to the rest of the world. In Ethiopia cash is still the most dominant medium of exchange and electronic-banking is not well known. There is a centralized bank called National Bank of Ethiopia. The sector is closed for non-Ethiopian citizens. Proclamation No.592/2008 does not allow foreigners to own and operate banks in Ethiopia. Hence presently there are no foreign banks operating in the country.

According to the National Bank of Ethiopia, at the end of fiscal year 2014, the number of banks operating in the country reached 19 of which 16 were private, and the remaining 3 state-owned. Information system has become the heart of modern banking in our world .the banking sector in Ethiopia is one of the rapidly growing sectors of the country's economy. During the fiscal year these banks opened 480 new branches raising the total branch network in the country to 2,208 from 1,728 year 2013.

Based on the NBE 2014 annual report, the significant branch expansion was undertaken by Commercial Bank of Ethiopia (CBE) with 124 branches, followed by Oromiya International Bank (44 branches), Awash International Bank (38 branches), Cooperative Bank of Oromiya

(31 branches), Dashen Bank and Bunna International Bank (30 branches each), Berhan International Bank (26 branches), and United Bank (24 branches) (NBE 2014 Annual Report).

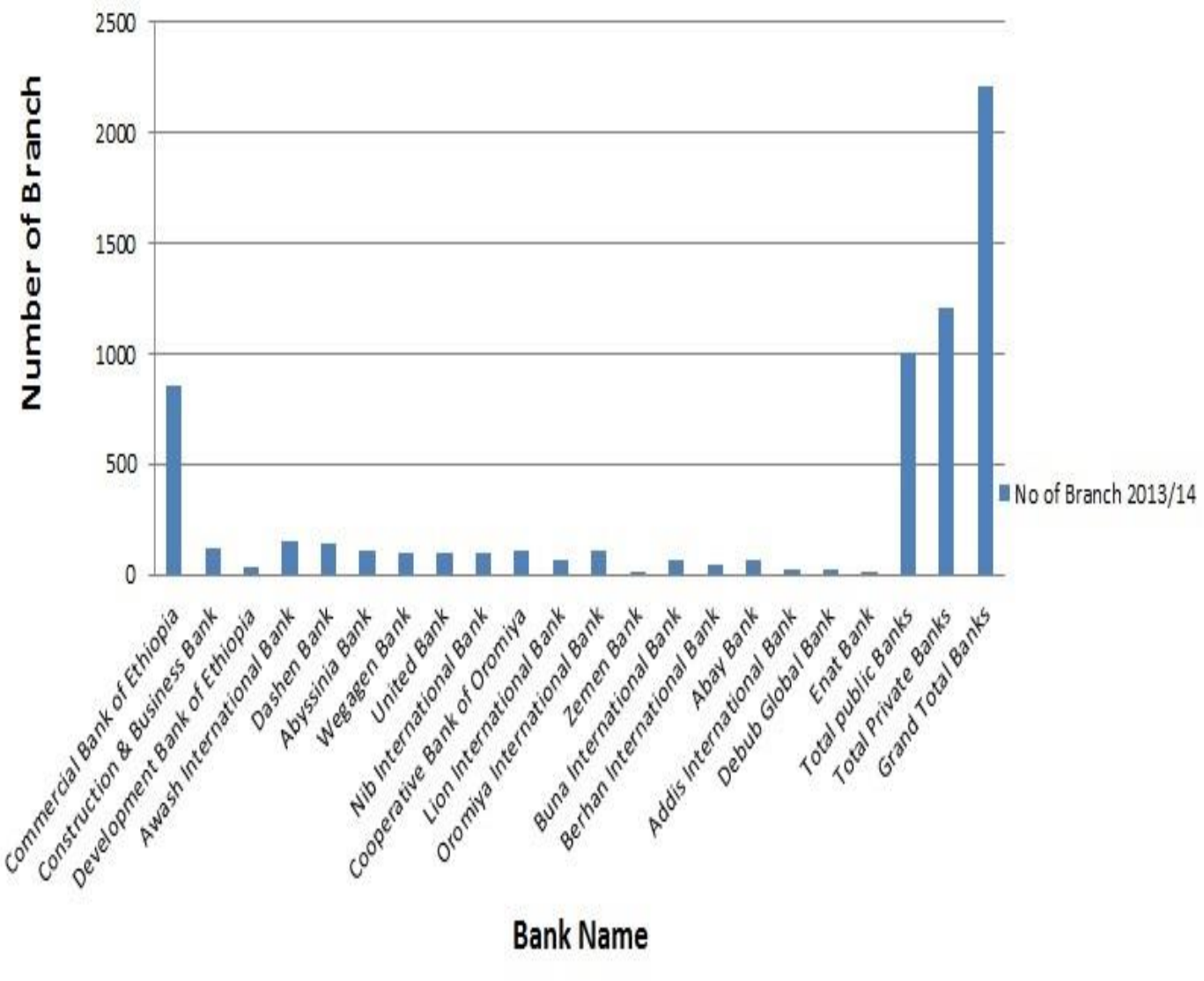


Fig.1.1: Branch distribution of the commercials banking industry in Ethiopia.

(Source: NBE 2014 Annual Report)

Currently, Ethiopian private commercial banks offer four major services in all of their branches. This includes Credit Facility, Saving Scheme, International Banking, and Fund Transfer. Moreover, some of the banks are also providing the customer's credit card payment systems that can be used internationally. The other service the banks render is deposit services

including demand deposit, savings deposit, youth savings deposit and time/fixed deposit (Simeneh, 2013).

Statement of the Problem

Failure of information security in terms of Confidentiality, Integrity and Availability (CIA) may result in many negative consequences such as loss of revenue, penalty, lost productivity and reputation loss. As a consequence, many banks invest to develop its information security system and maintain its effective information infrastructure. The insider threat is becoming quickly the biggest information security problem faced by the institutions. With access granted to the internal systems, and it became increasingly difficult to protect organizations from insider threats. PWC 2014 Global State of Information Security Survey, Employees are the most named culprits of security incidents. The great majority of intellectual property theft is committed by insiders.

Previous Surveys confirms and reveal that current or former employees are the second greatest cyber-security threat, exceeded only by hackers (Greitzer et al., 2008).It is difficult to rely on the technology that our banking industry have today people are the weakest link. We can have the best technology; firewalls, intrusion-detection systems, biometric devices and somebody can call an unsuspecting employee (Blackwell C, 2009) trusted insiders can attack our banking service any time with a catastrophe of higher magnitude.

Malicious insider threats pose a serious threat to organizations. The identification of malicious insider threats, however, is extremely difficult, expensive, error prone, and time consuming (Joseph S., et al, 2013). The insider threat has for far too long been overlooked by both government and non- government owned banks when conducting their risk and threat analysis assessments. Every organization it has diverse variety of consultants, employees, and partners, then it's difficult to protect form the insider threat. (Roy Sarkar, 2010). Problem from the insider threat it causes harm to the system or the organization more than any other threat.

Surveys confirms and reveal that current or former employees are the second greatest cyber-security threat, exceeded only by hackers (Greitzer et al., 2008).It is difficult to rely on the technology that our banking industry have today people are the weakest link. We can have the best technology; firewalls, intrusion-detection systems, biometric devices and somebody can call an unsuspecting employee (Blackwell C, 2009) trusted insiders can attack our

banking service any time with a catastrophe of higher magnitude.

Based on the 2007 CSI Computer Crime and Security Survey (R. Richardson, 2007), 59% of respondents reported that they had experienced insider abuse of network resources; 26% reported that over 40% of their total financial losses from cyber-attacks were due to insiders .The 2014 global economic crime survey , saying cyber-crime is a growing threat globally and the second most commonly reported economic crime affecting financial service firms (GECS, 2014).Many problems are the result of technology progress and business objectives. Business managers push to provide application and data access for customers and suppliers, but these users increase the risks associated with an insider attack.

The problem area driving this research to be conducted was the current state of Knowledge with regards to Insiders threat management within the Ethiopian banking industry almost null. The other influential actors influencing this thesis work to be study was the current problem that faced the Ethiopian banking industry, which was the misuse of information and other theft committed at different government and private banks by the trusted employees or insiders.

This study seeks to bring to the fore the need for a review of the insider threat to an Ethiopian banking sector. The insider threat has for far too long been overlooked by many bank managers and governing bodies; during conducting their risk and threat analysis assessments. Banks can suffer from direct effects, such as financial losses (Baker et al., 2008), but also from indirect effects. These indirect effects include, for example: risks to reputation that could dramatically impact share prices, or losing competitive advantage, due to loss of intellectual property (Sinclair and Smith, 2008).

One of the main reasons that the Ethiopian banking sector facing a problem from insider is that they cannot buy the honesty of the employees. Therefore the purpose of this study will be a catalyst and valuable reference for Ethiopian banking sector re-imagine their efforts in dealing with fraud and insider attacks.

Despite some very industrious research efforts, insider threat remains an area of research that still holds many unanswered questions. This assessment seeks to fill the gap in study, concerns and approaches relating to insider threat in Ethiopian banking industry. In order to determine a course of action going forward, a central research question was developed. The central research question stated simply was:

Q1.which insider threats are most prevalent for the Ethiopian commercial banking sector?

Q3. What are the motives behind insider's threats in Ethiopian banking industry?

Q2.What measures are currently in use to mitigate these insider security threats?

1.3 Objective of the Study

This survey work has a general objective and a list of specific objectives in order to solve the problems that initiate this study.

1.5.1 General Objectives

The objective of this study is to enhance the insider threat of the Ethiopian banking industry. It will allow the policy makers the opportunity to understand the problem, its magnitude and its potential consequences. More importantly, this survey result lays out a pathway to significantly reduce the vulnerability to banking services and increases the awareness of the threat presented by bank insiders.

This survey aim is to bring together the findings from a variety of perspectives on the insider threat in Ethiopian banking industry.

1.5.2. Specific Objectives

The reasons behind these assessment specific objectives were to identify and understand the threat that insiders posed to the Ethiopian banking sector. To assess those issues related to insider threat, the researcher focused on the insider threat, motives and mitigation strategies of the Ethiopian banking industry, the study will have the following specific objectives:

- To identify which insider threats are most prevalent in Ethiopian banking industry.
- To identify the motives behind insider threat in Ethiopian banking sector.
- To identify measures currently in use to mitigate insider security threats.
- To report analysis result and make recommendations.

1.4 Scope of the Study

From the entire financial sector operating in Ethiopia, the research covers particularly the activities of sixteen privately owned commercial banks and three state owned banks that are registered by NBE and become operational before the year 2013 / 2014as shown in (appendix

D).And the main focus area for this particular study lies on the current prevailed insider threats, motives and mitigation strategies of the insiders in the Ethiopian commercial banking sectors

1.6. Limitation of the study

In this survey all commercial banks operate in Ethiopia were included .This makes the outcome of the survey more compressive. However, due to time and financial constraint this research will focus on insider threat related with data collection, storage and distribution aspects of the Ethiopian banking industry. The National Bank of Ethiopia is not included because of the nature of the research focus on commercials banks.

The other limitation faced in conducting this research, all banks are no at same level of maturity in handling insider threats. This makes the data collection task a bit tough. There are no other major limitations encountered while undertaking this research.

1.7. Significance of the Study

This study seeks to fill the gaps in knowledge and approached relating to insider Information Security threats by analyzing the types of information security threats facing both the government and private banks in Ethiopia and the mitigation strategies to insider security threats. The study will also add to the body of knowledge in information security's studies by establishing the prevalent types of insider threats, mitigating strategies and challenges encountered in controlling insider threats within the Ethiopian banking services.

The output of this survey will allow policy makers to view the problem presented in a comprehensive yet uncomplicated manner. It will allow policy makers the opportunity to understand the problem, its magnitude and its potential consequences in Ethiopian banking industry. It may also serve as a starting point for researchers who want to conduct more comprehensive research in this area from Ethiopian banking sector perspective.

1.8. Organization of the Study

The paper is organized in five main chapters, the first chapter presents introduction which gives a general aim, coverage and scope and other basic issues of the paper. In the second chapter, literature review which includes related theoretical literature reviews in this chapter previous theoretical studies that are related with insider threat will be reviewed. The third chapter illustrates the methodology and data collection. The fourth chapter presents data analysis, interpretation and discussions of each research questions. The final chapter, which is chapter five, will be conclusions and recommendation. In this chapter some recommendations were made based on the study finding and the literature review.

CHAPTER TWO

2. LITERATURE REVIEW

The second chapter of this study examines in detail the notion of the term insider threats and provides an up-to-date overview of the currently employed techniques to protect these insiders in banking sectors and other related organization were assessed. Different financial institution and related sectors are currently faced with the problem of insider threats to their vital information assets. While insider threats pose a risk to both commercial and government organizations, the impact of such breaches in security on the financial or military side could be more damaging due to possible impacts in national security and foreign relations.

2.1. Insider

Who is an insider*?*

It is difficult to find a general standard definition for insider threat. This makes the task of insider threat study difficult. Aeran (2006) defined insiders as employees working within the organization. This, however, is the traditional definition of insiders. Insiders have the potential to cause major financial loss and damage to the reputation of an organization, particularly in the Banking and Finance Sector where transaction between consumers and other organizations occur almost every second(Tang L.,2005).

Burke and Christiansen (2009) define insiders as people with authorized and legitimate access to the organizations resources such as the corporate networks, applications, and data. The other common definition of an insider is given by Richardson; individual with privileged access to an IT system (Richardson, 2007).The term "insider" in information security behavioral research commonly refers to the users having access to the corporate information systems and knowledge of the organizational processes, which allow a wide range of information security behaviors including those that are disruptive, unethical or illegal (Willison and Warkentin, 2013).

Throughout this study, I use the definition:

> *An insider means potential, current or former employees or contractors who have legitimate access to information, techniques, technology, and information assets of the banks.*

2.2. Definition of Insider Threat

A threat is an unwanted event that may result in harm to an asset, often employing and exploiting known vulnerabilities (Randazzo et al., 2004).Threat is potential cause of an incident that may result in harm of systems and organization (ISO 27005).A threat is something that may or may not happen, but has the potential to cause serious damage.

Belford (2010) define an insider threat as the action of an insider that puts an organization's data, processes, or resources at risk in a disruptive or unwelcome way. Trzeciak (2009) defines insider threat as a current or former employee, a contractor or a business partner who has or had authorized access and intentionally exceeded that access in a manner that negatively affected the confidentiality, integrity or availability of the organization's information or information systems. Insider threats are trusted members of an organization who compromise security and are often cited as the greatest cyber security threat to organizations (Holmlund et al., 2011).

A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems(Cappelli et al.,2009).

Insider threat *means the threat posed by unauthorized access, use or disclosure of privileged information, techniques, technology, and assets of the banks by an individual with legitimate or indirect access, which may cause harm.*

This definition will better explain throughout this research.

Some of the impact of Insider activity within different originations can be:

Damage to:

- Reputation

- Relationships
- Buildings & assets

Disruption to:

- Processes & procedures
- IT systems

S. Prama et.al (2009) enumerates some example of insider threat as follows:

1. An insider can copy content of a document into another document
2. An insider can remember content and retype it in a lower classified document
3. An insider can get a dump of memory (such as the video buffer) and then print the document
4. A malicious insider can tamper with the existing rights on the document
5. An insider can misaddress an e-mail. To a wrong email group or person
6. An insider can make a typo in an e-mail address addressing it wrongly. Instead of J.doeP.doe gets the e-mail or by spelling mistakes a e-mail is send to a domain owned by the competitor for example you own .com and the competitor .net
7. An insider can read, copy, print and send a document he has access to unless fine grained access control is in place.
8. An insider can become owner of a document by copying it
9. An insider can forward a document to a person either inside or outside the organization
10. An insider can work after business hours when maybe detection systems are not running
11. An insider can become victim of phising

2.2.1. Categories of Insider Threat

Different researchers categorized insiders' threats in different ways. Cole, E., et.al. (2006) categorize insiders in to two, pure insider and Insider Associate. Pure insider is an employee who has all the rights and access associated with being an employee. This employee usually

has keys or a badge that allow them into the organization and user IDs and passwords that allow them access to the company's network. This is known as authorized 'privileged' access. The pure insider is the most dangerous type as they can cause the most damage to the organization based on their access. Insider Associate Insider associates are people such as contractors, the cleaning crew, or security guards who have limited authorized access to your facility or network. They are not company employees and don't need full access to organization's network (Cole, E., et.al, 2006).

Tom C. (2014) views the insider threat as three distinct categories and I preferred this categorization for this specific study:-

1. **Negligent Insiders** - Insiders who accidentally expose data – such as an employee who forgets their laptop on an airplane
2. **Malicious Insiders** - Insiders who intentionally steal data or destroy systems – such as a disgruntled employee who deletes some records on his last day of work.

Some security institutes again divide malicious insiders in two types (CPNI, 2014).

> *Self-motivated insiders* are individuals whose actions are undertaken of their own volition, and not initiated as the result of any connection to, or direction by, a third party
>
> *Recruited insiders* are individuals co-opted by a third party to specifically exploit their potential, current or former privileged access. This includes cultivates and recruited foreign intelligence, or there entities with malicious intent,

3. **Compromised Insiders** - Insiders whose access credentials or computers have been compromised by an outside attacker

Insiders have a critical point of preference in hurting an organization. Insiders can sidestep efforts to establish safety, physical and specialized, introduced to avoid unapproved access. Technological measure, for example, firewalls and interruption recognition are utilized to for the most part guard against external threat. In addition, they have knowledge of policies,

procedures, and technologies used in their organizations, and are often also knowledgeable about vulnerabilities (Chinchani, 2005).

Insider fraud incidents cases were usually detected the result of a tip rather than an audit or through the use of other detection strategies (Association of Certified Fraud Examiners, 2008). This is true for Ethiopian banking sector too. Most of the time the case is detected after a couple of days or after the employee left the bank. Similar findings were reported by Porter (2003) who found that the majority of insider fraud was detected by either a tip or by accident. These findings suggest that the number of cases of such fraud that are officially reported is only a lower bound estimate of the actual figure.

According to the CSO MAGAZINE, USSS, CERT, and Deloitte(2013) Survey, 46% of the respondents considered the maleficence caused by insider attacks as more damaging than those caused by outsider attacks. Chinchani et al (2005) argue that several challenges are associated with the insider threat and claim that security administrators consider the insider threat as unpreventable. Insiders have a higher success rate with maleficence not only because they are familiar with security controls, but also because most tools are aimed at neutralizing external threats. The motivations of malicious insiders range from apathy to espionage, sabotage, terrorism, embezzlement, extortion, bribery, corruption and ignorance the motivations of malicious insiders range from apathy to espionage, sabotage, terrorism, embezzlement, extortion, bribery, corruption and ignorance(K. Nance and R. Marty,2011).

There are a small number of insider studies that have had a substantial impact on enhancing our current level of knowledge of observable insider impact within the financial sectors. Although the studies all revolve around the problem of insider threat, most of them focus more on preventative measures that may reduce the threat of an attack.

Base on the current Vormetric Insider Threat study report, globally 89% of respondents felt that their organization was now more at risk from an insider attack; 34% felt very or extremely vulnerable. When the researcher asked about who posed the biggest internal threat to corporate data, a massive 55% of respondents said privileged users, nine percentage points behind on 46% were contractors and service providers, and then business partners at 43%. Databases, file servers, and the cloud hold the vast bulk of sensitive data assets, but for many (38%) mobile is perceived as a high-risk area of concern (Vormetric, 2015).

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.

In the study by Randazzo et al. it became clear that in almost 9 out of 10 cases of insider incidents, insiders used easy, legitimate user commands to trigger an incident. There is no standard profile of an inside attacker. Only 23% of them hold technical positions and most of them have no history of hacking whatsoever (Randazzo et al., 2004).

Information security management framework for banking industry in Ethiopia (kelem T, 2013) is already done. He attempts to improve the overall information security management of the banking industry. His focus area includes both the internal and external information security threats. But when we see the current trends of the information security crimes or attacks in Ethiopian banking industry comes from insiders. This makes me focus our research area on those issues related to insider threats.

2.3. Insider Threats Motives

It is important to try to understand why certain individuals commit insider attacks, and a number of studies have explored the motivating forces driving these illegal behaviors (Agata M., et.al, 2012). There is generally no single or simple reason for an employee deliberately seeking to cause harm. Commonly, malicious trusted insiders have a number of motives for their activity .Motivations is complex and often mixed. Those who betray their organization are often driven by a mix of personal vulnerabilities, life events and situational factors.

Financial gain was the greatest motivator for the attackers (Josephine W., 2012). Insider attacks for financial gain is a growing area of concern for banks, and a growing source of income for bad employees with access to valuable information, because theft and fraud-related attacks are primarily motivated by financial gain. Other motivations included revenge, dissatisfaction, or a desire for respect. Some of the insiders who stole confidential or proprietary information were also disgruntled and motivated by revenge (Willison, 2009).

Based on the US Secret Service and CERT Coordination Centre, Insider Threat Study,

Perpetrators did not share a common profile. Most of the insiders did not hold a technical position, did not have a history of holding in hacking activities and were never perceived as a problem. Insiders ranged from 18 to 59 years of age, majority of them single (52%) and male (58%) and came from a variety of racial and ethnic backgrounds (CERT, 2004).Some other goals, separate from motivation, included deliberate information system sabotage and stealing proprietary information (Randazzo et al., 2005). Some of the insiders who stole confidential or proprietary information were also disgruntled and motivated by revenge (Willison, 2009).

Cappelli et al. (2006) found that although some of these individuals were motivated by money, debt and drug related problems, the vast majority of them did not have a financial need, nor were they disgruntled or dissatisfied with their employer. Therefore, their motivations remain unclear and difficult to categories and understand. The majority of cases of IT sabotage occurred as a direct result of employment suspension or termination (Moore et al., 2008).In prior research ideology is less common motive, the terrorist insider threat may be a real threat to the power grid, and other critical infrastructure.

Albrechtsen, (2008) agrees that it would be foolish to neglect employees as a possible malicious threat. Mitnick and Simon (2002) identifies a number of these scenarios such as the use of social engineering to attack information systems by getting hackers to manipulate people by using social techniques to perform the actions they desire. The most perplexing group of insiders was those who committed acts of fraud. Cappelli et al. (2006) found that although some of these individuals were motivated by money, debt and drug related problems, the vast majority of them did not have a financial need, nor were they disgruntled or dissatisfied with their employer.

Cappelli, and Trzeciak (2008) presented a dynamic-system model of the insider IT sabotage problem, where the insider's main aim is to harm some parts of the organization, such as business operations, information and the system or network. Their model too, mostly focused on one primary problem, and they did not consider other types of insider threats, such as fraud or the stealing of sensitive information .Disgruntlement is another reason for an individual to turn hostile.

A study by Moore, Cappelli and Trzeciak (2008) was able to take the results of the study conducted by Cappelli et al. (2006) and delve further into the threat of insider IT sabotage. In

this study, the authors outline seven predominant observations that were common in cases of insider IT sabotage. The first three observations relate directly to the psychological, behavioral and situational factors that were present, while the other observations are organizational and technical limitations that unintentionally helped to facilitate a successful attack (Moore et al., 2008).

2.4. Mitigating the Insider Threat

The insider incidents being on the rise, most companies are initiating steps to safeguard against a possible insider attack. Various approaches have been employed and discussed on how to counter and combat insider threats. Most of these approaches are reactive and involve dealing with insider threat after the damage has been done which is too late.

Josephine W. (2012) technical approaches have limitations in that they fail to identify malicious insider activities that appear as legitimate tasks. The research confirms that successful defense against insider threats depends on both technical and behavioral solutions (Martinez-Moyano et al., 2008). Technical controls include mechanisms to protect information systems from attacks or incidents. Antivirus software, access controls, backups, recovery and audit software, for example (Melara et al., 2003).Management must pay close attention to many aspects of the organization, including IT business policies and procedures, organizational culture, and technical environment (Silowashetal., 2012).

It is difficult to protect insider threat only by information security policy alone. Kirlappos etal. (2013) argued that centralized policy may not fit with local and situational events that demand greater flexibility to cope with information security risks, thereby suggesting the employees to be trusted in making own decisions to mitigate the insider threat.

Managing insider threats using threat assessments is documented in one aviation management journal (Randazzo, 2008).Another area addressing insider threat_methods are those derived from technological solutions. A diverse array of technological solutions such as biometric systems, surveillance, and tracking are on the market and well documented.

Different research programs have been utilized to mitigate an insider attacks to information system infrastructures before they occur. These programs are designed to identify security breaches (Sobh, 2005). Thus, their main goal is to spot intrusions on information or in a network. To mitigate the insider threat, Colwill (2010, p. 193) suggests a four-point

approach combining (1) encryption, (2) access control, (3) minimum privilege, and (4) monitoring, auditing and reporting. Unfortunately, research has shown that there is a gap between security awareness and execution of security plans (Colwill, 2010).

Fischer (2008) suggests that organizations have appropriate programs in place to assist vulnerable employees. If employees are experiencing any form of personal crisis or difficulty, it is recommended that employees are encouraged to use employee Assistance Programs. The feedback provided by the perpetrators of acts of espionage delivered the strong message that early intervention may have prevented the act occurring in the first instance (Fischer, 2008).

The Insider Threat Security Reference Architecture (ITSRA) provides an enterprise-wide solution to insider threat. (Moore, 2012) .The architecture consists of four security layers: Business, Information, Data, and Application. Organizations should deploy and enforce controls at each layer to address insider attacks. The ITSRA draws from existing best practices and standards as well as from analysis of these cases to provide actionable guidance for organizations to improve their posture against the insider threat.

The ITSRA consists of four distinct layers as highlighted above and shown in figure below. The first layer, the Business Security layer contains high-level business Requirements, such as an organization's mission and also involves the creation of policies, procedures, and other guidance that determines the level of security to be implemented in other layers.

Layer 2 or the Information Security layer describes the organization's information infrastructure including the network and associated components such as routers, switches, and servers. This layer also contains the operating systems and software required to manage the infrastructure.

Layer 3 or the Data Security layer involves information assets considered to be owned exclusively by the organization such as documents, spread sheets, or databases.

The final layer called the Application Security layer addresses both the development of software that contribute to the organization mission by ensuring that policies defined at the Business Security layer are enforced

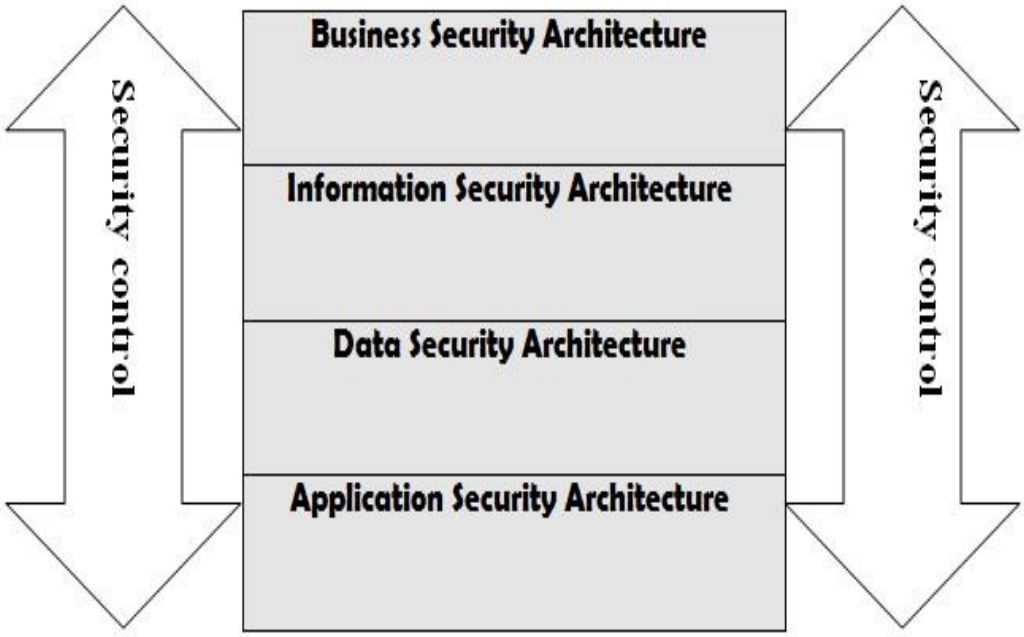


Figure 2.1: Insider Threat Security Reference Architecture (Montelibano & Moore, 2012).

Role-based access control (RBAC) is used to specify policies for tasks, called roles, in the organization rather than individual users (Chandramouli, et al, 2003).The users get assigned to roles in order to gain access to resources. The assignment of users to roles follows some constraints such as the "principle of separation of duty", role hierarchy, etc. RBAC provides an advantage that will reduce the inconsistencies that arise when policies have to be specified for subjects individually. The role-based access control does not address any information flow restrictions. Temporal Role Based Access Control (TRBAC), an extension of RBAC, also specifies time constraints on when a role can be enabled or disabled (E. Bertino et al, 2001).For example, a constraint stating that a document cannot be opened beyond normal office hours can be specified in TRBAC. We go beyond temporal analysis and consider other factors such as machine's IP address

The insider threat research conducted by Kowalski et al. (2008) does suggest that insider attacks occur after careful consideration and preparation, with the majority of insiders planning their attack in advance. This research indicated that, in the majority of cases, behavioral warning signs were observable prior to an attack. Observable behaviors of

concern included absenteeism, arguments with co-workers and poor performance, and in 70% of cases, individuals were actually reprimanded for inappropriate behaviors in the workplace (Kowalski et al., 2008). Kowalski and associates recommend that in these situations access rights should be reviewed for individuals who are displaying any behavior that is deemed to be threatening to the security of the organization. This response may prevent the successful completion of an attack.

Hu, Bradford and Liu (2006) developed a model for detection of insider attacks by intrusion detection systems based on the assumption that an insider is described by job function. However, the influence of social insider factors was not considered in this model. Currently there is no complete solution since any security measures put into place, whether by policy or technology, require the user have legitimate access to the system at some level.

2.4.1. Best Practices for Managing Insider's Security Threats

Gartner recommends taking a multifaceted approach to mitigating the Insider Threat. They say combine high-tech, low-tech and "no tech" approaches to provide defense in depth (Gartner, 2008).he put the following

Implement No-Tech and Low-Tech Security Measures

- Implement pre-employment screening.
- Enhance the security awareness program.
- Find out who has the "Keys to the Kingdom."
- Update policy and compliance requirements. Enforce policies and procedures.
- Audit for compliance.

Implement your current high tech security tools and identify gaps

- Intrusion prevention systems which are strategically placed at various points inside the perimeter.
- Database Activity Monitoring Tools
- Identity Administration Tools

In addition, Gartner recommend everyone's to evaluate and implement controls that are appropriate to their enterprise's technical environment, corporate culture, regulatory environment, risk profile, business needs and other enterprise-specific factors.

The second best practice provides the most current recommendations from the CERT Program, part of Carnegie Mellon University's Software Engineering Institute, based on an expanded database of more than 700 insider threat cases and continued research and analysis. They include mappings of each Best Practice to the International Organization for Standardization (ISO) 27002:2005. Furthermore, each practice lists several recommendations that organizations of various sizes should implement immediately to mitigate (prevent, detect, and respond to) insider threats (Cappelli, D.M.et al., 2012).

For the purpose of this guide, a malicious insider is defined as a current or former employee, contractor, or business partner who meets the following criteria:

Table 2.1: Best Practices Mapped to Standards

Practice Number	Best Practice	ISO 27002
1	Consider threats from Insiders and business partners in enterprise-wide risk assessments.	·Identification of risks related to external parties ·Addressing security when dealing with customers ·6.2.3 Addressing security in third party agreements
2	Clearly document and consistently enforce Policies and controls.	·15.2.1 Compliance with security policies sand standards
3	Incorporate insider threat awareness into periodic security training for all employees.	·8.2.2 Information security awareness ,education ,and training
4	Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.	·8.1.2 Screening
5	Anticipate and manage Negative issues in the work environment.	·8.2.1 Management responsibilities ·8.2.3 Disciplinary process ·8.3.1 Termination responsibilities
6	Know your assets.	·7.1.1 Inventory of assets
7	Implement strict Password and account management policie sand practices.	·11.2.3 User password management ·11.2.4 Review of user access rights
8	Enforce separation of Duties and least privilege.	·10.1.3 Segregation of duties ·11.2.2 Privilege management

9	Define explicit security Agreements for any cloud services, especially access restrictions and monitoring capabilities.	·Identification of risks related to external parties ·Addressing security in third party agreements ·10.2.1 Service delivery ·10.2.2 Monitoring and review of third party services ·10.2.3 Managing changes to third party services
10	Institute stringent access controls and monitoring policies on privileged users.	·10.10.4 Administrator and operator logs ·10.10.2 Monitoring system use
11	Institutionalize system change controls.	·10.1.2 Change management
12	Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.	·10.10.1 Audit logging ·10.10.2 Monitoring system use
13	Monitor and control Remote access from all end points, including mobile devices.	·11.4.2 User authentication for external connections ·11.7.1 Mobile computing and communications
14	Develop a comprehensive Employee termination procedure.	·8.3.1 Termination responsibilities ·8.3.2 Return of assets ·8.3.3 Removal of access rights
15	Implement secure backup and recovery processes.	·10.5.1 Information back-up
16	Develop a formalized Insider threat program.	·6.1.2 Information security coordination ·15.1.5 Prevention of misuse of information processing facilities
17	Establish a baseline of normal network device Behavior.	
18	Be especially vigilant Regarding social media.	
19	Close the doors to Unauthorized data infiltration.	·12.5.4 Information leakage

Source:*(Software Engineering Institute Carnegie Mellon University, CERT common sense guide to prevention and detection of insider threat 2012)*

In summary, Most of the research reported on insider threats covers the problem from the researcher's individual perspective, focusing on one primary problem seen as either a technical or human factor. A recent study however, indicated that successful protection against internal threats relies on both technical and behavioral solutions (Munshi et al, 2012).

2.5. Security Awareness on insider threats

Most organizations are not even aware of the insider threat problem. The majority of insiders do not consider the consequences of their actions when undertaking an attack. Educating employees about the consequences of such attacks from the perspective of both the business and the perpetrator may act as a deterrent to such attacks.All banks should give their employee proper awareness training. Training provided to employees should address insider threats that exist to the company. Employee should be made aware of the bank's security policy and required to sign the policy document with its copy issued to them for future reference. Each employee should be made aware of its access rights so that no unauthorized resources are accessed accidentally (Aeran, 2006).

Security training may change the value of beliefs, add beliefs regarding security, or modify current beliefs. In literature, for instance, security education has been shown to influence beliefs of intrinsic benefit, safety, rewards, work impediment, intrinsic cost, vulnerability, and sanctions (Bulgurcu et al., 2010). Training has also been shown to help employees realize how vulnerable their organization is to security threats (Siponen et al., 2009). When employees learn to behave securely through training, these beliefs will influence attitude and ultimately behaviour.

2.6. Challenges of Insider Threats

Banking sector in Ethiopia faces numerous challenges adopt advanced technologies as well as E-banking applications and seize the opportunities.

Insider threat is misperceived. Organizations often concentrate on external attacks. Almost all security audit tools and modeling techniques are readily available which aid in studying vulnerabilities of studying external threats. On the other hand, insider threat is not correctly perceived because it is difficult to measure it. Insider threat is a low base rate problem. Perpetrators of insiders' attacks are users with legitimate authorization, and therefore, it is difficult to predict or protect against these attacks. Consequently, security officers view these attacks as unpreventable, resulting in failure to act.

Lack of Suitable Legal and Regulatory Framework in managing insider threats Ethiopian current laws do not accommodate electronic contracts and signatures. Ethiopia has not yet enacted legislation that deals with E-commerce concerns including enforceability of the

validity of the electronic contracts, digital signatures and intellectual copyright and restrict the use of encryption technologies. ICT in Ethiopia is now collaborating with Europe and other countries in the world and developing regulatory frame work for banking sector.

Insider threat is high impact. Although insider attacks may not occur as frequently as external attacks, they have a higher rate of success, can go undetected and pose a much greater risk than external attacks. This is due to the fact that insiders enjoy certain important advantages over external adversaries. They are familiar about their targets and the security countermeasures in place.

Most organizations believe that their current (technical) security measures are able to stop most insider attacks. These organizations need a reality check: a security program/policy can reduce the risk of an insider attack to an adequate level, but only if the employees have a certain level of security awareness (Randazzo et al., 2004).

Insider attacks are unpredictable. Actually, most inside attacks are planned in advance and thus can be prevented. In practice, specific signs that are signaling an attack usually go unnoticed or are ignored. Large number of cases show planning behavior or frustration on the part of employees beforehand and many of the (intentional malicious) inside attackers had committed less serious violations prior to their actual attack.

One of the challenges here in Ethiopia in protecting insider attack is the ISP .In Ethiopia there is one ISP which provide a connection between banks with its own branch .this creates a huge obstacle in their day to day activities.

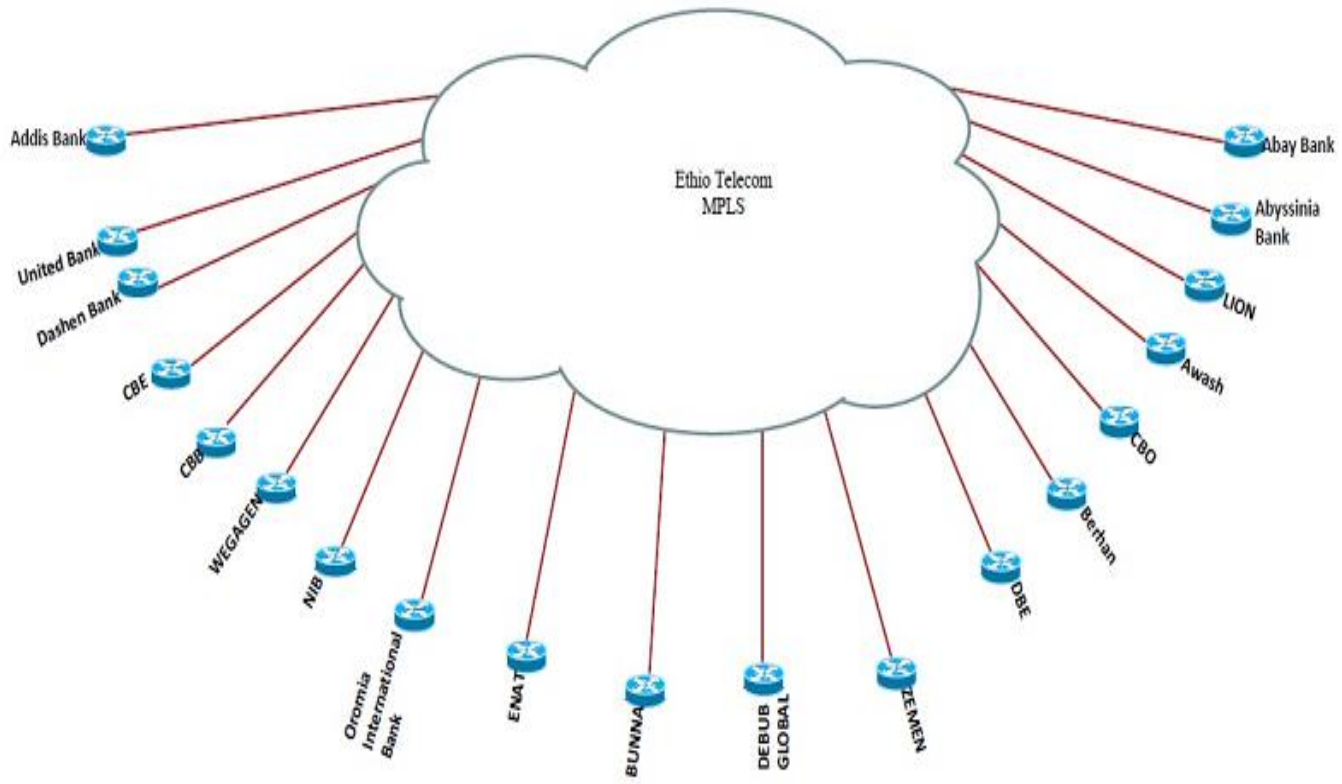


Figure 2.2: Ethiopian commercial banks connection with ethio telecom multiprotocol label switch (MPLS) vpn connection.

Combating Insider Threat is multidisciplinary challenges. People have a tendency to think that IT is solely responsible for all computer security issues. IT cannot address insider threat by itself. Are policies in place? Are they realistic? Does legal support IT practices? This kind of question always answered by the legal department of the given bank or organization. Concerning HR this department may be responsible for who is coming and going? Who has work place issues and similar scenarios were addressed by this department. In Ethiopian banking industry almost all bans have a legal department or legal directorate.

2.7. Role of People in Protecting Insider's Threats

People are important resources in the information security activities of an organization. Researchers have recently discovered, however, that employees are largely an untapped resource for protecting organizational information assets (Albrechtsen and Hovden 2009; Dlamini et al., 2009).The heart of any information security is people. Within organizations employees play a vital role in information security. Employers need to be especially attuned to any financial problems that their staff may be experiencing as these can precipitate an

attack. This is particularly important because research has shown financial gain to be a strong motivating factor in some cases of insider attack (Kowalski et al., 2008). People are considered the weakest link in the security chain. Awareness of the risks and available safeguards is the first line of defense for security of information.

Employees are confident to challenge others if they are not complying with security requirements. One of the biggest threats to information security is not the latest variation of some new malware that exploits technical vulnerabilities, rather, the malicious actions or inadvertent errors of trusted employees (Pironti, 2013) that operate 'inside the firewall' (Warkentin and Willison, 2009).so organization to invest on people in protecting their resource from possible insiders. Many researchers argue that people are the first line of defense, but they are also are the main cause of security breaches (Angell and Pironti, 2013; Samonas and Angell, 2010; Samonas, 2012).

People use computers for everything from banking and investing to shopping and communicating. An information security culture is needed so as to protect all banks assets from insider's security breaches. Prevention includes educating people about the value of information and increasing people's awareness about security threats. If an authorized user tells another person his secret code, the unauthorized user can masquerade as the authorized user with significantly less likelihood of detection.

There are observable personality characteristic that may be common to individuals who commit malicious acts and comparatively rare in other employees (Moore et al., 2008). System administrators or other employees with special privileges also pose a greater risk since they have access beyond traditional employees. I believe all employees of both the government and private banks have to be treated with equal suspicion and that proper mechanisms are put in place to prevent information security breaches by all employees. All staff should be encouraged to be vigilant and attentive to any threats that other employees may make against the organization. Any threats or boasts that individuals may express concerning harm to the company should be treated seriously and investigated (Cappelli, Moore, Trzeciak and Shimeall, 2009).

The previous studies on insider threats have focused on different aspects of insider threats, like types of insiders, challenge in mitigating insiders, insider attack, characteristics of insiders, and different mitigation strategies proposed by different researchers. But it is

difficult to find or achieve a clear and common mitigation strategies .the nature and a characteristic of insiders varies from business to business.

During this study literature review, it is difficult to find any local research that is specifically focus on insider threat. Many of the researchers that has been done so far focused on intrusion detection, external attacks and other related areas only. This shows that in the Ethiopian banking industry, knowledge of the dominant type of insider threat will be essential to enable the bank in controlling the consequence of insider attacks. This study also helps other government organization and non-government organization to see their current drift in mitigating their insider threat prior to any malicious attack.

CHAPTER THREE

3. Research Methodology

Redmen and Mory (2009) explain Research Methodology as a method used to collect information and data for the intention of making business decisions which may consist of surveys, interviews and other research methods. In other words, this is where the researcher tries to defend or search the given questions thoroughly, his or her own way until answers and conclusions are gotten. They also explain research as a systematized effort to gain new knowledge while Goddard and Melville (2004) described research as answering unanswered questions or exploring which currently not exist is a research.

3.1. Research Design

Research design can be defined as the logical plan to interrelate research question to gathered data, and the interpreting and conclusions to be drawn (Yin, 2003). The research design is the first part of the empirical research methodology. A survey research method is employed in order to assess the insider security threat in the banking sector in Ethiopia. The survey was conducted among banks that are active in the in Ethiopia financial services sector. The survey is an appropriate means of gathering information under three conditions: when the goals of the research call for quantitative and qualitative data, when the information sought is specific and familiar to the respondents and the researcher has prior knowledge of the responses likely to emerge. (Ronald Jay P, 2005).

Regardless of the sensitive nature of the information that was asked for in the survey, the number of participants to the survey was high, with a total of 18 surveys returned only one respondent deny to return the questionnaire. Additionally, some people sent me some additional general information on how they think about certain information security issues and how their security was implemented in their banks. However, this high response rate was already expected and the results that did come back were very useful and helped to create some insight in how the financial services sector copes with their insider threat.

3.2. Population of the Study

A primary data is collected from headquarters of three government and sixteen private commercials banks headquarters which were found at the capital city of Ethiopia, Addis Ababa. A Census approach was used and all the representatives of the entire population (the respondents) were targeted. The questionnaires responses were handled with utmost confidentiality.

3.2.1 Determination of the Sample Design

There are two kinds of surveys: sample surveys and census surveys. In a sample survey, data are collected for only a fraction (typically a very small fraction) of units of the population while in a census survey; data are collected for all units in the population. Two types of sampling exist: non-probability sampling and probability sampling. Non-probability sampling provides a fast, easy and inexpensive way of selecting units from the population but uses a subjective method of selection. In order to make inferences about the population from a non-probability sample, the data analyst must assume that the sample is representative of the population. This is often a risky assumption given the subjective method of selection.

Probability sampling is more complex, takes longer and is usually more costly than non-probability sampling. However, because units from the population are randomly selected and each unit' probability of selection can be calculated, reliable estimates can be produced along with estimates of the sampling error and inferences can be made about the population. Since non-probability sampling is usually inappropriate for a statistical agency, this manual focuses on probability sampling.

3.3. Data Collection

3.3.1 Instruments of Data Collection

The quality of the research tool will inevitably determine the quality of information collected. The question were carefully designed in addressing the basic research objectives and most of the question is adopted from 2013Vormetric/ESG Insider Threats Survey, US CERT program survey on insiders threats, GECS 2013 insider threat study and others research and researcher question which helps in conducting insider threat survey in different organizations. The questionnaires were tested during pilot study .almost all of the questions were used by

different international data security organization like U.S. Secret Service, *CSO Magazine*, Price Waterhouse Cooper, and Cyber security Watch Survey as a standard in assessing a given organization insider threat.

3.4.1. Questionnaire

A questionnaire was categorized in to three the parts; such as Demographic information, insider threats, and Mitigations. As shown in (Appendix A), the questions items are open and closed on practices and status in insider threat. The questioners were prepared and distributed to senior IT security staffs of the respective Banks.

The questionnaires were tested during pilot test. Some of the question that requires clarity was modified .Add some explanation to some questions. Questions like categories of insiders were modified based on the pilot test. On the other hand, question that probes the amount of damage in terms of birr was omitted. This question believed to be a negative impact on the reputation of a given bank. Many of the questions that the researched adopted were serving as questionnaires by different researchers and security research institutes.

Five-point Likert scale survey was developed to collect IT personnel perceptions on the current insider threat of Ethiopian commercial banking sectors. The scale's descriptors were placed into five groups: "No extent at all", "little extent", "moderate extent", "great extent" and "very great extent". The items represented various employee insider issues that have been described as important to business operations.

3.4.2 Documents

Different documents are revised and assessed for this specific study. Printed materials; books, journal articles, NBE annual reports, magazines published INSA and conference proceedings, and internet sources were used to know the subject area in depth, and assess other countries experiences in insider threats management specifically in their financial sectors.

3.2.2 Sampling Method

For this specific study the researcher preferred a non-probable purposive sampling. Purposive sampling refers to situations where participants are selected based on their specialized insight or special perspective, experience, characteristic, or condition that the student researcher wish

to understand (Yegidis, L. & Weinbach ,W. ,1996) .It suit to attain the study objective. All employee didn't Fit this study, identify those staffs that are responsible or have ample knowledge of the respected bank ICT security and insider threat related tasks. Then the questionnaires were distributed to this staffs purposefully.

3.5 Pilot Study

It is necessary to conduct a pilot study in order to assess the relevance of the instruments designed to collect data for the study. According to connely (2008), extent literature suggests that a pilot study sample should be 10 % of the sample projected for larger parent study The pilot study was conducted in two of the sample Banks (Oromia international bank and Awash international bank) which is 10.5 % of the total sample size. The aim was to find out and avoid ambiguity, omissions and misunderstanding of each item. Using the relevant comments from results of the pilot study and suggestions of the advisor corrections was made.

3.6 Reliability and Validity

In order to determine whether the questionnaire that used to collect the data is reliable or not, internal consistency of each section of the questionnaire were tested using cronbach alpha. The figure below shows the reliability is high. Concerning the validity I meet with my advisor in person and with telephone conversation for a couple of times to check the validity of this study.

The Analysis and finding of this study was discussed in the National Bank of Ethiopia, with bank supervisions directorate staffs .This discussion help the junior researcher to conform the validity and importance of the study.

Reliability test result of the Questionnaires		
Section of the Questionnaire	**Cronbach's Alpha**	**N of items**
Insider threat	.929	21
Motivation	.930	16
Mitigation	.977	24
Behavior(characteristics)	.959	23
Challenge	.895	11

Table 3.1: The reliability of each section of the questionnaires using cronbach's alpha.

CHAPTER FOUR

4. Data Analysis, Interpretation and Discussions

This Chapter is divided into three sections: Section one which relates to demographic information of the population, Section Two which focuses on nature of Insider threats facing Ethiopian banking sector and Section Three which covers the mitigation strategies currently implemented by those government and private banks.

This chapter analysed and discusses all the research objectives based on the primary data collected from the questionnaires. There were a total of 18 respondents who represented a total of 18 different commercial banks out of the available 19 commercial banks as at the time of the research.

The study covered 94.73 % of the population under research, and has the double benefit of enhanced credibility of the findings and strengthened the conclusions.

$$\frac{\text{Number of completed questionnaires}}{\text{Number of questionnaires sent out}} = \frac{18}{19} \times 100 = 94.73\%$$

This shows that the response rate is high and it could be considered valid for proceeding with the analysis of data obtained.

4.1. Demographic

4.1.1. Gender

Table 4.1 Gender distribution of the respondents

		Frequency	Percent	Valid Percent
Valid	Male	16	88.9	88.9
	Female	2	11.1	11.1
	Total	18	100.0	100.0

Data on gender were collected from the 18 respondents, the data was analyzed and the outcomes were as presented as percentages in Table 4.1. Interestingly the respondents were 2 women and 16 men.

This flags the gender appropriation in the field of bank insider threat administration and data security as seen from the Ethiopian banking industry viewpoint alone. This information may

be useful in drawing conclusions about the gender distribution in the field of information technology security issue in a general sense. There is a huge discrepancy between men and women in administration of threat within the banking industry.

4.1.2. Age of Participants

Table 4.2 Ages of the participants

		Frequency	Percent	Valid Percent
Valid	25-30	1	5.6	5.6
	31-35	5	27.8	27.8
	36-40	6	33.3	33.3
	41-45	3	16.7	16.7
	46 and above	3	16.7	16.7
	Total	18	100.0	100.0

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 33.3%. Only 5.6% were below the age of 30 and majority of them were below 40 years.

4.1.3. Position

Table 4.3: position of the participants

		Frequency	Percent	Valid Percent
Valid	Director	1	5.6	5.6
	IT manager	7	38.9	33.3
	chief information officer	2	11.1	11.1
	senior network administrator	2	11.1	5.6
	others	6	33.3	44.4
	Total	18	100.0	100.0

The objective of this question was to ensure that the information provided was given by a person knowledgeable enough to know about the insider threat and security mitigation factors used in the respected bank they represented. Most of the respondents were mainly in charge of information security management while the others had an information security technical role.

4.1.4. Experience

Table 4.4: Experience of the participants

		Frequency	Percent	Valid Percent
Valid	below 5 years	8	44.4	44.4
	6-10	5	27.8	27.8
	11-15	2	11.1	11.1
	16-20	3	16.7	16.7
	Total	18	100.0	100.0

From table 4.4 the highest numbers of participants, which are 44.4%, have an experience of below 5 years. This may show there might be a high turnover of a bank employee who is working related to ICT security. If there is a high turnover of employees in a given organization, it is liable for cyber security attack.

4.1.5. Number of Employees

Table 4.5: Number of employees in your bank

		Frequency	Percent	Valid Percent
Valid	below 50	2	11.1	11.1
	51-500	1	5.6	5.6
	501-1000	5	27.8	27.8
	1000-5000	8	44.4	44.4
	above 5000	1	5.6	5.6
	Missing	1	5.6	5.6
	Total	18	100.0	100.0

4.1.6. Number of Branches

Table 4.6: Number of branches owned by banks

		Frequency	Percent	Valid Percent
Valid	11-30	3	16.7	17.6
	51-70	2	11.1	11.8
	71-100	4	22.2	23.5
	above 100	8	44.4	47.1

	Total	17	94.4	100.0
Missing	System	1	5.6	
	Total	18	100.0	

44.4 % of the participant of this research confirmed that their bank has a branch of above 100. According to the National bank Ethiopia, at the end of fiscal year 2014, the number of bank branch reaches 2208.so whenever there is an expansion of branch is made ICT security should be always in consideration. There are issues raised during branch expansions. Like resource mobilizations and others.

4.1.7. Average Age of Perpetrators

Table 4.7: The average age in years of the perpetrators of insider threats encountered the bank

		Frequency	Percent	Valid Percent
Valid	below 25	3	16.7	33.3
	25-30	5	27.8	55.6
	31-35	1	5.6	11.1
	Total	9	50.0	100.0
Missing	System	9	50.0	
	Total	18	100.0	

55.6% of insider cases occurred within the 25-30 years age category. Instance of insider cases increased with age until they peaked within this category and then decreases beyond 35 years of age .here all the respondents are not willing to answer the given question.

Based on the participant figure, most of the perpetrators within the Ethiopian banking fall at age below 30.so the bank should consider age in assigning a person for the position of ICT security and related infrastructure positions.

4.1.8. Percentage of Central IT Budget

Table 4.8: Percentage of the central IT budget estimate spent on information security

	Frequency	Percent	Valid

				Percent
Valid	less than 1%	2	11.1	12.5
	1-5%	6	33.3	37.5
	5-10%	2	11.1	12.5
	10-15%	4	22.2	25.0
	greater than 15%	2	11.1	12.5
	Total	16	88.9	100.0
Missing	System	2	11.1	
Total		18	100.0	

From the table 4.8 about 37.5 % the respondents' falls an IT budget of 1 -5 % of the total IT budget is allocated in fighting the possible information threat.

4.2. Result

4.2.1. Insider Threat

In order to collect a data about insider threat from respondents, 23 likert scale questions which with five agreement levels (1= Not extent at all, 2= Little extent, 3= Moderate extent, 4= Great extent and 5= Very great extent) were administered.

Table 4.9: Insider threats that challenges information security of banks

N^{o}	Insider threats	Not extent at all		Little extent		Moderate extent		Great extent		Very great extent		mean
		n	%	n	%	n	%	n	%	n	%	
1	Destruction of critical data	9	50	5	28	2	11					1.5625
2	Theft of critical information like bank customers records and business plan	8	44	5	27	2	11	2	11			1.8824
3	Financial fraud	2	11	10	55.6	2	11	1	5.6	1	5.6	2.3125
4	Spoofing(pretending to be something or someone that one is not)	10	55.6	5	27.8			3	16.7			1.7778
5	Computer virus implantation	7	39	6	33.3	2	11	1	5.6	1	5.6	2.0000
6	Social engineering (manipulation of users to obtain formation)	7	39	6	33.3	3	16.7	1	5.6	1	5.6	2.0556
7	Installation of unauthorized software	2	11	5	27.8	4	22.2	5	27.8	2	11	3.0000
8	Purposefully installing malicious software	14	77.8	2	11	2	11					1.3333

9	Impersonation of other users	8	44.4	9	50			1	5.6			1.6667
10	Sabotage (disrupting operations, network)	9	50	6	33.3	2	11	1	5.6			1.7222
11	Tampering with data (unauthorized changes of data or records)	7	39	8	44.4	1	5.6	2	11			1.8889
12	Unauthorized Access	10	55.6	5	27.8	1	5.6	1	5.6	1	5.6	1.7778
13	Organized Crime(Insiders colluding with criminal gangs)	13	72.2	4	22.2	1	5.6					1.3333
14	Identity Thieves(Impersonation Fraudsters)	11	61	6	33.3			1	5.6			1.5000
15	Activists(to bring social or political change through actions)	14	77.8	4	22.2							1.2222
16	Password Cracking	8	44.4	7	39	1	5.6	1	5.6			1.7059
17	Phishing (acquiring information and/or money from people without their knowledge)	9	50	7	39	2	11					1.6111
18	Key loggers(hardware or software- based, they capture keystrokes)	12	66.7	5	27.8	1	5.6					1.3889
19	Selling employer's confidential information to the competitor(s)	10	55.6	4	22.2	3	16.7					1.3889
20	Malicious programs or Trojan horse programs were installed on company assets	5	27.8	8	44.4	4	22.2	1	5.6			2.0556
21	Attempt to attach hardware peripherals to desktop systems without authorization	8	44.4	6	33.3	2	11	1	5.6	1	5.6	1.9444

To determine extent of the insider threat that are faced by banks in Ethiopia, data collected from 18 banks were analyzed using frequency distribution, percentage and mean. As indicated in table 4.9, about 38.8% (m= 3) of the respondents claimed that Installation of unauthorized software should be considered as an internal threat for information security of banks.

Additionally, 22.2% of them reported that Installation of unauthorized software as a moderate internal threat for the information security of banks.

Some of the insider threats such as financial fraud (m=2.31), Malicious programs or Trojan horse programs were installed on company assets (m= 2.05), Computer virus implantation (m=2) Social engineering (manipulation of users to obtain formation) (m=2.05) and Attempt to attach hardware peripherals to desktop systems without authorization (1.94) had little effect on the information security system of the banks.

The mean score of the rest insider threats including destruction of critical data, Theft of critical information like bank customers records and business plan, Spoofing(pretending to be something or someone that one is not),Purposefully installing malicious software, Impersonation of other users, Sabotage (disrupting operations, network), Tampering with data (unauthorized changes of data or records), Unauthorized Access, 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), and Selling employer's confidential information to the competitor(s); is ranged from 1.22 to 1.88 that means from little extent to no extent at all. As shown in the (Appendix C). Standard deviations of each response's participants distribution is spread very closely around the mean response allowing for accurate conclusion inferences.

Regardless of the extent, the following insider threats have been existed from very little extent to very great extent. See the fig below here **"N"** represent the number of respondent out of 18

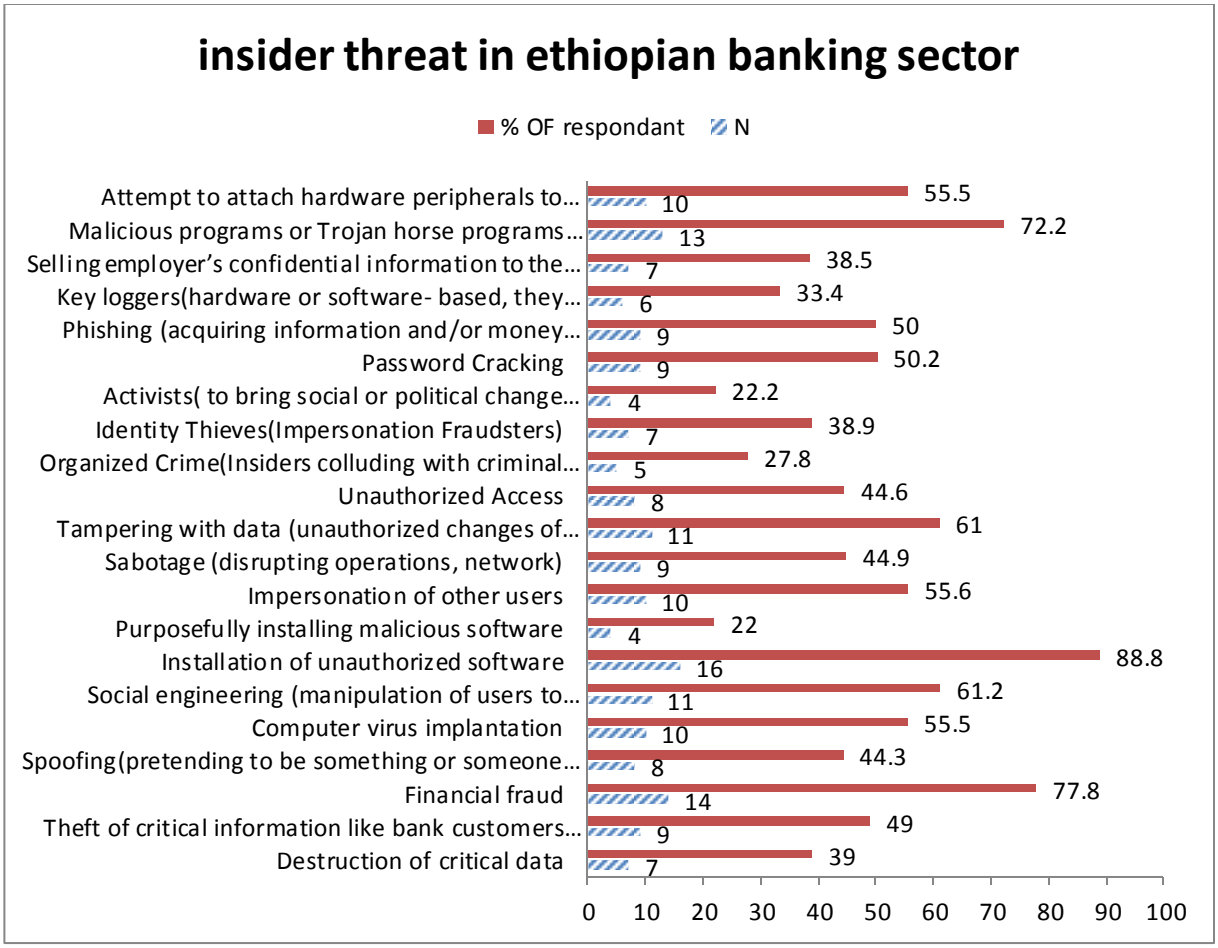


Figure.4.1: Insider threats in Ethiopian banking sector (excluding no extent at all).

4.2.2. Types Of Insiders

Table 4.10: Types of insiders

N^{o}	Types of Insider	Not extent at all		Little extent		Moderate extent		Great extent		Very great extent		mean
		n	%	n	%	n	%	n	%	n	%	
1	Negligent Insiders	8	44.4	8	44.4	-	-	2	11			1.7778
2	Malicious Insiders	11	61	5	27.8	2	11					1.5000
3	Compromised Insiders	13	72.2	4	22.2	1	5.6					1.3333

Respondents were asked to identify which type of insiders is manifested (experienced) in their banks.

As indicated in table 4.10, none of the types of insiders manifested in the banks in a significant extent. But, negligent insiders were observed in a few manner (m=1.77), whereas,

malicious and compromised insiders are not exhibited almost in all banks (m= 1.5 and 1.33 respectively).

4.2.3.Behaviors Or Characteristics Displayed

Table 4.11: Behaviors displayed by insiders.

N^{o}	Behaviors	Not extent at all		Little extent		Moderate extent		Great extent		Very great extent		mean
		n	%	n	%	n	%	n	%	n	%	
1	Remotely accesses the network while on vacation, sick or at odd times	10	55.6	7	39	1	5.6					1.5000
2	Uncharacteristic comments made to co-workers	10	55.6	4	22.2	3	16.7					1.5882
3	Unnecessarily copies material, especially if it is proprietary or classified	8	44.4	6	33.3	3	16.7	1	5.6			1.8333
4	Drop in performance and/or attendance	8	44.4	4	22.2	4	22.2					1.7500
5	Interest in matters outside of the scope of their duties	4	22.1	9	50	3	16.7	1	5.6	1	5.6	2.2222
6	Have Criminal tendencies	15	83.3	3	16.7							1.1667
7	Have a reduced sense of loyalty	7	39	8	44.4	2	11	1	5.6			1.8333
8	Social transgression tendencies	11	61	5	28	2	11					1.5000
9	High ethical flexibility	7	39	5	28	5	28					1.8824
10	Emotional distress	7	39	7	39	4	22.2					1.8333
11	Resistance to authority	8	44.4	4	22.2	5	27.8					1.8235
12	Lack of empathy (disregard for the impact of other peoples actions)	6	33.3	6	33.3	4	22.2	1	5.6			2.0000
13	Introversion(often loners)	8	44.4	7	39	1	5.6	1	5.6			1.7059
14	Mostly depressed	8	44.4	6	33.3	2	11	1	5.6			1.7647
15	Frustration with the workplace	7	39	5	28.7	4	22.2	2	11			2.0556
16	Across system usage patterns(Unusual system usage patterns)	9	50	7	39	2	11					1.6111
17	Making of Meaningful errors	10	55.6	4	22.2	4	22.2					1.6667
18	Deliberate markers (leave small,	12	66.7	4	22.2	2	11					1.4444

	intentional signs)											
19	Weakness in handling conflicts	6	33.3	10	55.6	2	11					1.7778
20	Curiosity to learn systems both operations and technical	5	27.8	4	22.2	6	33.3	2	11	1	5.6	2.4444
21	Have Tendencies to work extended hours and preferably late nights and weekends	4	22.2	5	27.8	4	22.2	3	16.7	2	11	2.6667
22	Obsessive tendencies (continuously preoccupied)	6	33.3	6	33.3	5	27.8	1	5.6			2.1111
23	Imitation and modeling those whom they respect	10	55.6	5	27.8	2	11	1	5.6			1.6667

To determine which behavior (characteristics) displayed by insider, 23 Likert scale questions with five level agreement were administered. Employees who have the curiosity to learn systems, both operations (m= 2.44) and techniques, and who have tendencies to work extended hours and preferably late nights and weekends (m= 2.66) are likely a characteristic manifested by insiders within the Ethiopian banking industry at moderate extent.

On the other hand, having a characteristics such as unnecessarily copies material (1.83), especially if it is proprietary or classified (m=1.75), drop in performance and/or attendance, Interest in matters outside of the scope of their duties (m=2.22), have a reduced sense of loyalty (m=1.83), high ethical flexibility (m= 1.88), emotional distress (1.83), lack of empathy (disregard for the impact of other peoples actions) (m= 2), introversion(often loners) (m= 1.7), mostly depressed (m=1.76), frustration with the workplace (m=2), Weakness in handling conflicts (m=1.77) and obsessive tendencies (continuously preoccupied) (m= 2.1) are considered as a little extent to the organizations. The rest behaviors are not explained in Ethiopian banking sector.

4.2.4. Motivation

Table 4.12: Motivations that pushes employees to engage as threat

N^{o}	Motivations	Not extent at all		Little extent		Moderate extent		Great extent		Very great extent		mean
		n	%	n	%	n	%	n	%	n	%	
1	Steal data for monetary gain	7	38.9	4	22.2	2	11	4	22.2			2.17

	(stealing or manipulating financial details for personal monetary benefits)											
2	Disrupt critical systems for ideological reasons	15	83.3	1	5.6	1	5.6	1	5.6			1.4444
3	Dissatisfaction with bank's policies	9	50	4	22.2			3	16.7			1.8333
4	Dissatisfaction with immediate reporting manager	7	38.9	7	38.9	3	16.7	1	5.6			1.8889
5	Desire for recognition	5	27.8	6	33.3	5	27.8	2	11			2.2222
6	Disgruntlement (Frustrated employee will think of harming the company).	10	55.6	6	33.3			2	11			1.6667
7	Espionage(spy or mole that is influenced by criminals or competitors targeting the bank)	11	61	6	33.3	1	5.6					1.4444

N^{o}	Motivations	Not extent at all		Little extent		Moderate extent		Great extent		Very great extent		mean
		n	%	n	%	n	%	n	%	n	%	
8	Quest for challenge(explore the world around or take it a challenge)	10	55.6	4	22.2	3	16.7	1	5.6			1.7222
9	Revenge(employees with negative feelings towards the company or individuals within the company)	10	55.6	6	33.3	1	5.6	1	5.6			1.7222
10	Emotional distress(Employee is highly frustrated)	8	44.4	5	27.8	2	11	2	11			1.8824
11	Sabotage(of company operations)	13	72.2	3	16.7	2	11					1.3889
12	Theft(data stored in computer hard ware and software, company or customer financial data)	12	66.7	5	27.8	1	5.6					1.3889
13	Curiosity (experimenting with company's network resulting in disruption of services)	11	61	5	27.8	2	11					1.5000
14	Hooliganism (such as defacing a Website)	11	61	6	33.3	1	5.6					1.4444
15	Family problems	10	55.6	4	22.2	3	16.7	1	5.6			1.7222
16	Challenge security professionals	10	55.6	5	27.8	1	5.6	2	11			1.7222

In order to identify the motivations that lead employees to threat information security of the Ethiopian banking sector, 16 questions that have five level agreement likert scale questions were distributed for participants. As indicated in table 4.12, none of the motivating factors were reported as a great extent threat to the organizations. Some of the motivations -desire for recognition (m=2.22, 33.3%), Steal data for monetary gain (m=2.17, 22.2 %), dissatisfaction with immediate reporting manager (m= 1.88, 39%) and emotional distress (Employee is highly frustrated)(m=1.88)were identified as a motivations that has little extent. The rest motivating factors were considered as little extent to no extent at all.

Regardless of the extent at which each motives appeared, the following four motives prevailed in majority of banks. These are Emotional distress (Employee is highly frustrated), Steal data for monetary gain (stealing or manipulating financial details for personal monetary benefits), Dissatisfaction with immediate reporting manager and Desire for recognition we can visualize this from the following figure.

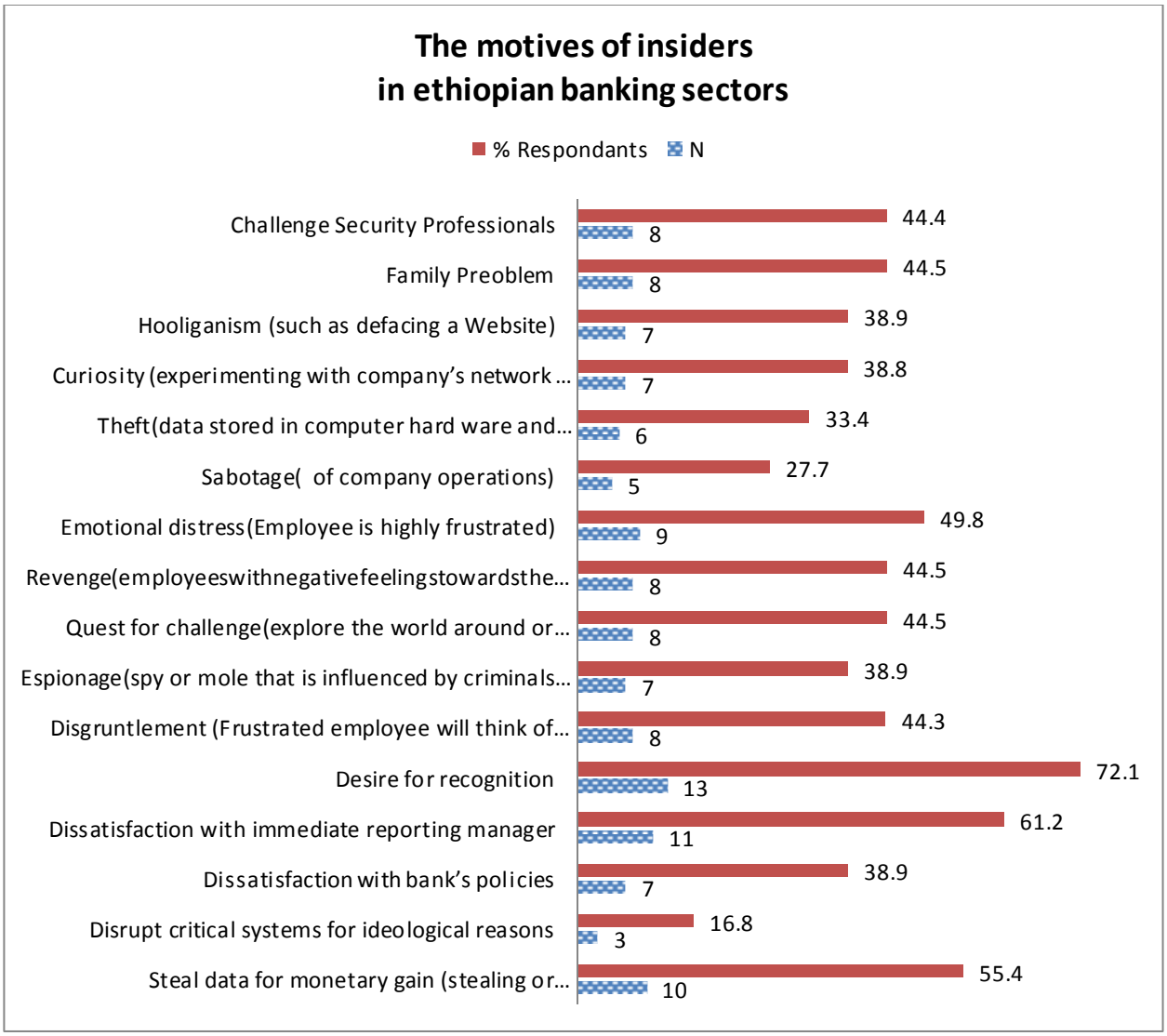


Figure.4.2: The identified motives behind insider threats in Ethiopian banking industry (excluding no extent at all).

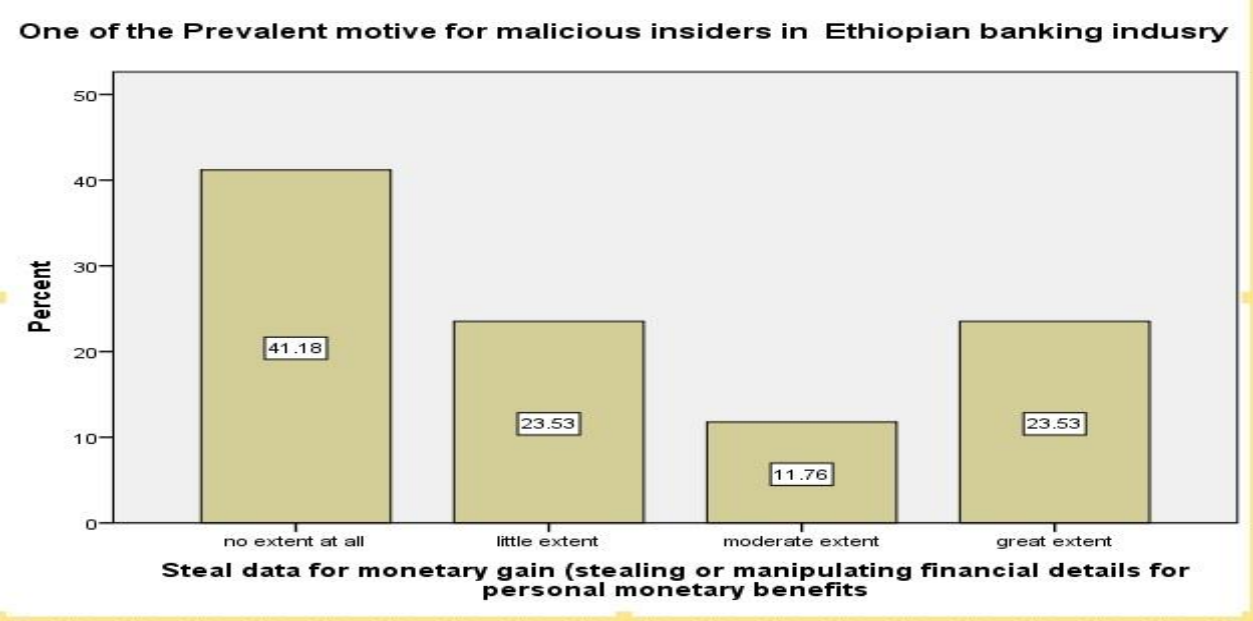


Figure 4.3. The motives of insiders: for monetary gain

The most perplexing group of insiders was those who committed acts of fraud. Cappelli et al (2006) found that although some of these individuals were motivated by money. other research finding shows that More than 27% of insiders studied stated that they were experiencing financial difficulty when the incident occurred (Randazzo, M.et al., 2005).like these and other previous researches finding, financial motive was one of the motives that prevailed during this study of insider threat in Ethiopian banking industry.

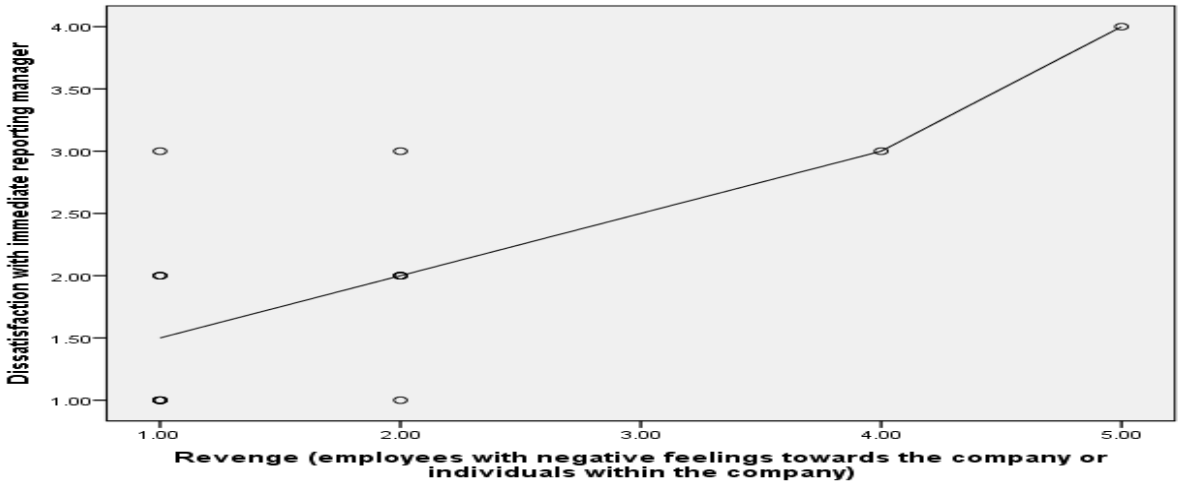


Figure 4.4: The relationship between dissatisfaction with immediate reporting manager and Revenge motives in Ethiopian banking industry.

There is strong relationship between these two motives: dissatisfaction with immediate reporting manager and Revenge motives in Ethiopian banking industry.

4.2.5. Mitigation Strategies

Table 4.13: mitigation strategies to prevent insider threat

N^{o}	Mitigation strategies	Not extent at all		Little extent		Moderate extent		Great extent		Very great extent		mean
		n	%	n	%	n	%	n	%	n	%	
1	Develop an insider incident response plan	3	16.7	3	16.7	5	27.8	4	22.2	3	16.7	3.0556
2	Periodic security awareness training for all employees	1	5.6	5	27.8	6	33.3	4	22.2	2	11	3.0556
3	Separation of duties and least privilege	1	5.6	3	16.7	5	27.8	4	22.2	4	22.2	3.4118
4	Strict password and account management policies			4	22.2	4	22.2	6	33.3	4	22.2	3.5556
5	Secure physical environment			1	5.6	6	33.3	7	39	4	22.2	3.7778
6	Deactivate computer access following termination			2	11	6	33.3	7	39	3	16.7	3.6111
7	Consider threats from insiders and business partners in enterprise-wide risk assessment	1	5.6	4	22.2	7	39	4	22.2	2	11	3.1111
8	Contracted service organizations or third party agree to abide by designated security and confidentiality policies.	3	16.7	5	27.8	3	16.7	3	16.7	3	16.7	2.8824

N^{o}	Mitigation strategies	Not extent at all		Little extent		Moderate extent		Great extent		Very great extent		mean
		n	%	n	%	n	%	n	%	n	%	
9	Use of layered defence against remote attacks	1	5.6	1	5.6	7	39	5	27.8	4	22.2	3.5556
10	Log, monitor and audit employee online actions			6	33.3	4	22.2	4	22.2	4	22.2	3.3333
11	Use of extra caution with privileged users			7	39	4	22.2	3	16.7	4	22.2	3.2222
12	Anticipate and manage negative workplace issues	1	5.6	4	22.2	5	27.8	7	39			3.0588
13	Consider secure coding in SDLC	1	5.6	5	27.8	4	22.2	4	22.2	3	16.7	3.1765
14	Implement system change controls removal.	1	5.6	4	22.2	6	33.3	4	22.2	1	5.6	3.0000
15	Implementing secure backup and recovery processes			1	5.6	6	33.3	3	16.7	6	33.3	3.8750
16	SIEM or other log analysis	4	22.2	2	11	5	27.8	1	5.6	4	22.2	2.9375
17	Monitor and respond to suspicious or disruptive behavior	1	5.6	5	27.8	7	39	2	11	3	16.7	3.0556
18	Tracking and securing of the physical environment (e.g. CCTV systems)			1	5.6	8	44.4	5	27.8	4	22.2	3.6111
19	Use of Data Loss Prevention suites (Restrictions on removal media like flash disks, CDs, etc.)	2	11	2	11	4	22.2	6	33.3	4	22.2	3.4444
20	Stringent Service Level Agreements with third party service providers	4	22.2	4	22.2	7	39	1	5.6	2	11	2.6111
21	Warning of all staff to be alert to anyone asking for sensitive or restricted information	1	5.6	5	27.8	5	27.8	3	16.7	4	22.2	3.2222
22	Establishing a formal grievance procedure for staff to vent their feelings	3	16.7	4	22.2	5	27.8	4	22.2	2	11	2.8889
23	Setting up an easy and confidential system for staff to	5	27.8	3	16.7	2	11	5	27.8	3	16.7	2.8889

	report any abnormal behaviors from their colleagues											
24	Work together across the Bank(increase all staff participation)	1	5.6	3	16.7	6	33.3	3	16.7	5	27.8	3.4444

According to table 4.13, some strategies such as Strict password and account management policies (3.55), Secure physical environment (3.77),Deactivate computer access following termination (3.61), Use of layered defense against remote attacks (3.55), Implementing secure backup and recovery processes (3.87), Tracking and securing of the physical environment (e.g. CCTV systems) (3.61), Use of Data Loss Prevention suites (Restrictions on removal media like flash disks, CDs, etc.) (3.44) were reported as have great and very great extent to protect the information security of the organizations from insider threats.

The rest of the strategies such as Develop an insider incident response plan, Periodic security awareness training for all employees, Separation of duties and least privilege, Consider threats from insiders and business partners in enterprise-wide risk assessment, Contracted service organizations or third party agree to abide by designated security and confidentiality policies, Log, monitor and audit employee online actions, Use of extra caution with privileged users, Anticipate and manage negative workplace issues, Consider secure coding in SDLC, Implement system change controls removal, SIEM or other log analysis, Monitor and respond to suspicious or disruptive behavior, Stringent Service Level Agreements with third party service providers, 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 behaviors from their colleagues, Work together across the Bank (increase all staff participation) scored the mean ranges from 2.6 to 3.44. So, they are considered as mitigation strategies that managers of banks should give moderate priority to implement.

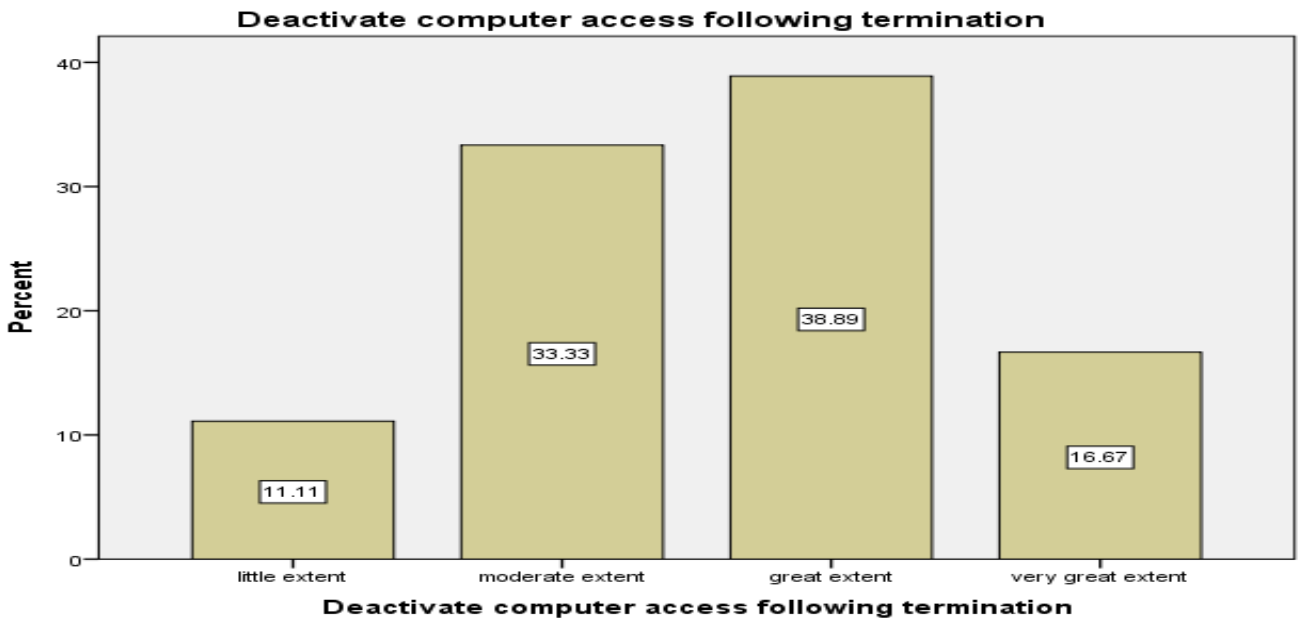


Fig 4.5 Deactivate computer access following their employee termination

Deactivate computer access following employee termination was one of the mitigation strategies mostly implemented in Ethiopian banking sectors.

Figure 4-5 shows that 55.56% of surveyed banks deactivate computer access following their employee termination with great and very great extent. In addition, 11.11% of the surveyed banks have implemented this mitigation strategy in little extent. The HR department or directorate of every bank should communicate the information system directorate when a given bank employee write a resignation letter. Deactivate computer access following termination. When an employee terminates employment, whether the circumstances were favorable or not, it is important that the banks have in place a rigorous termination procedure that disables all of the employee's access points to the bank's physical locations, networks, systems, applications, and data. The termination of a given employee should be communicated to all department or directorate of that specific bank.

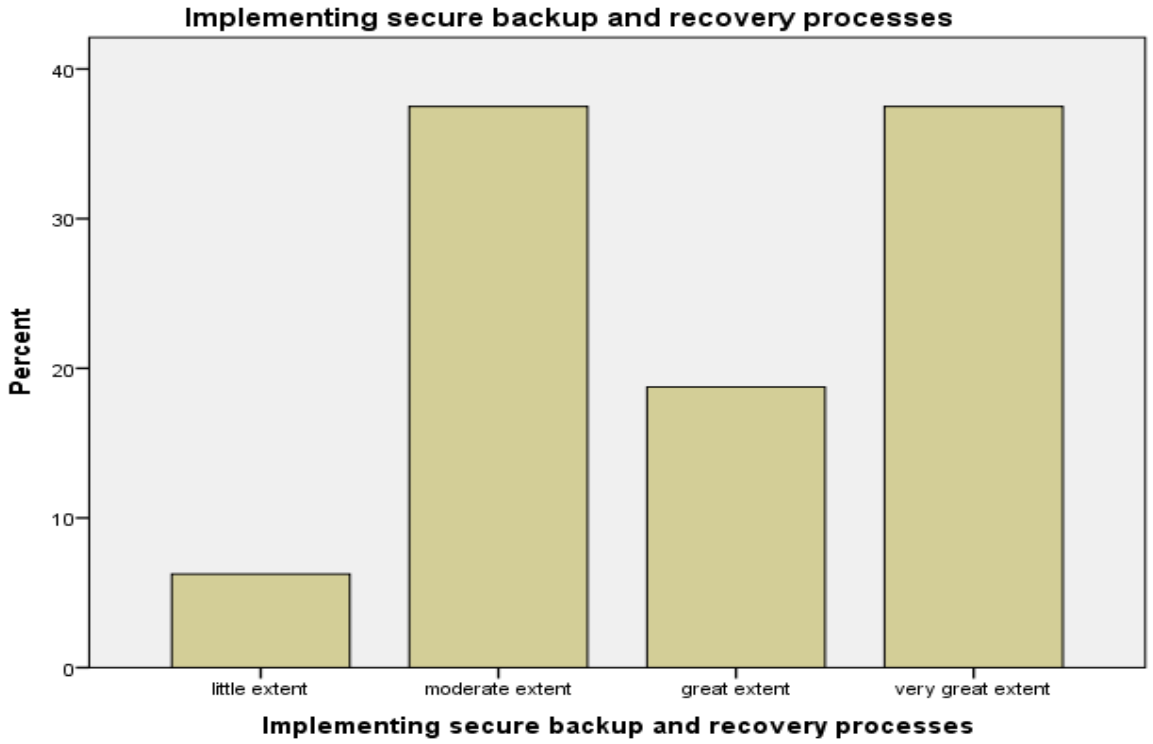


Fig 4.6: Implementation of secure backup and recovery in Ethiopian banking industry.

Prevention of insider attacks is the first line of defense. However, experience has taught us that there will always be avenues for determined insiders to successfully compromise a system. Effective backup and recovery processes need to be in place and operational so that if compromises do occur business operations can be sustained with minimal interruption (Moore et al, 2012). Our research has shown that effective backup and recovery mechanisms affected the outcomes in actual cases, and can mean the difference between

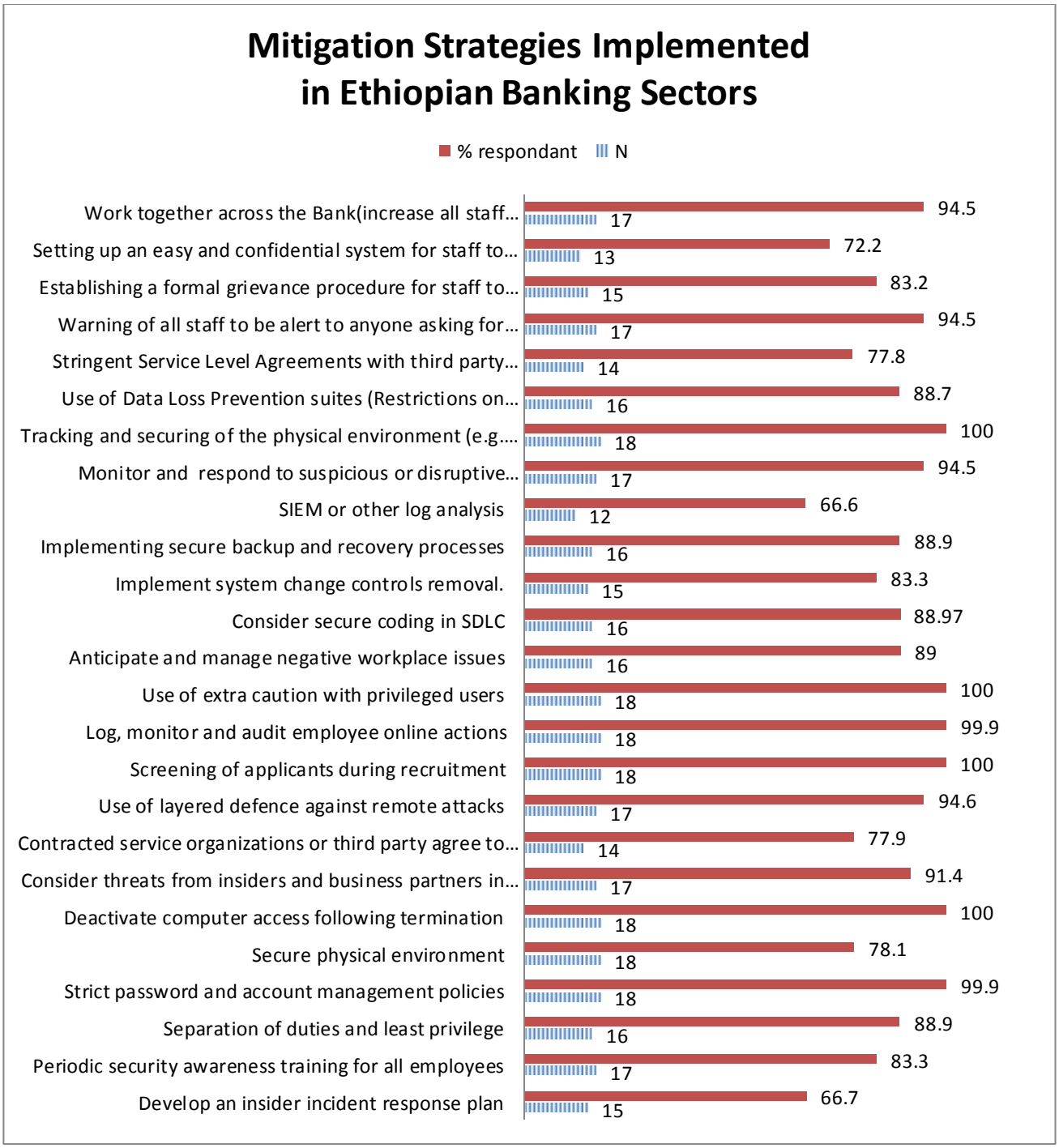


Figure 4.7: Mitigation strategies implemented from little extent to very great extent (excluding no extent at all).

4.2.6. Challenges

Table 4.14: Challenges the banks faced

N^{o}	Challenges	Not extent at all		Little extent		Moderate extent		Great extent		Very great extent		mean
		n	%	n	%	n	%	n	%	n	%	
1	Lack of research on insider threat	2	11	2	11	2	11	6	33.3	6	33.3	3.6667
2	Lack of education and awareness about insider threats			5	27.8	7	39	5	27.8	1	5.6	3.1111
3	Unavailability to specific technology solutions	3	16.7	4	22.2	3	16.7	6	33.3	1	5.6	2.8824
4	Lack of technical experience in using Security tools	2	11	4	22.2	9	50	2	11	1	5.6	2.7778
5	Lack of Suitable Legal and Regulatory Framework in regulating insiders threats.			4	22.2	5	27.8	7	39	1	5.6	3.2941
6	Vendor/Contractor management Issues	1	5.6	3	16.7	8	44.4	5	27.8	1	5.6	3.1111
7	Lack of information sharing	1	5.6	8	44.4	4	22.2	5	27.8			2.7222
8	Insufficient Audit trails			4	22.2	9	50	4	22.2			3.0000
9	Technology advancement increasing Opportunities for insiders	3	16.7	5	27.8	4	22.2	5	27.8	1	5.6	2.7778
10	Complexity of the security tools	3	16.7	6	33.3	3	16.7	2	11	3	16.7	2.7647
11	Jobs tress due to work load pressure	3	16.7	4	22.2	5	27.8	5	27.8	1	5.6	2.8333

To know the challenges that the banks faced while they are trying to implement mitigation strategies in order to establish a proper information security system, thirteen questions with five scales of agreement were administered. As shown in table 4.14, most of the respondents (66.6%) said that lack of research on insider threat has a great and very great extent.

Similarly, some of the challenges such as Lack of education and awareness about insider threats, Unavailability to specific technology solutions, Lack of technical experience in using Security tools, Lack of Suitable Legal and Regulatory Framework in regulating insiders Threats, Vendor/Contract or management Issues, Insufficient Audit trails, Job stress due to work load pressure considered as moderate challenges for Ethiopian banking industry.

Correlation

Here is the correlation among each section of the questionnaires .It was shown in (Appendix C) how this computed using SPSS

Correlations

		ethio banking industry insider threat	ethio banking industry insider challenge	ethio banking industry insider motive	ethio banking industry mitigation
ethio banking industry insider threat	Pearson Correlation	1	.707*	.733**	.211
	Sig. (2-tailed)		.010	.007	.585
	N	14	12	12	9
ethio banking industry insider challenge	Pearson Correlation	.707*	1	.597*	-.148
	Sig. (2-tailed)	.010		.040	.665
	N	12	14	12	11
ethio banking industry insider motive	Pearson Correlation	.733**	.597*	1	.243
	Sig. (2-tailed)	.007	.040		.472
	N	12	12	15	11
ethio banking industry mitigation	Pearson Correlation	.211	-.148	.243	1
	Sig. (2-tailed)	.585	.665	.472	
	N	9	11	11	12

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

Table 4.15: Pearson Correlation of each section of the questionnaires

- There was weak correlation between mitigation strategies and challenges. Here it indicates that if there is a good mitigation strategies implemented by the bank, there should be a reduction of challenges in protecting those insider threats.
- There was strong correlation between threat and behavior of the insider.

- There was also strong correlation between the motives of insider with the behavior manifested on his/her.

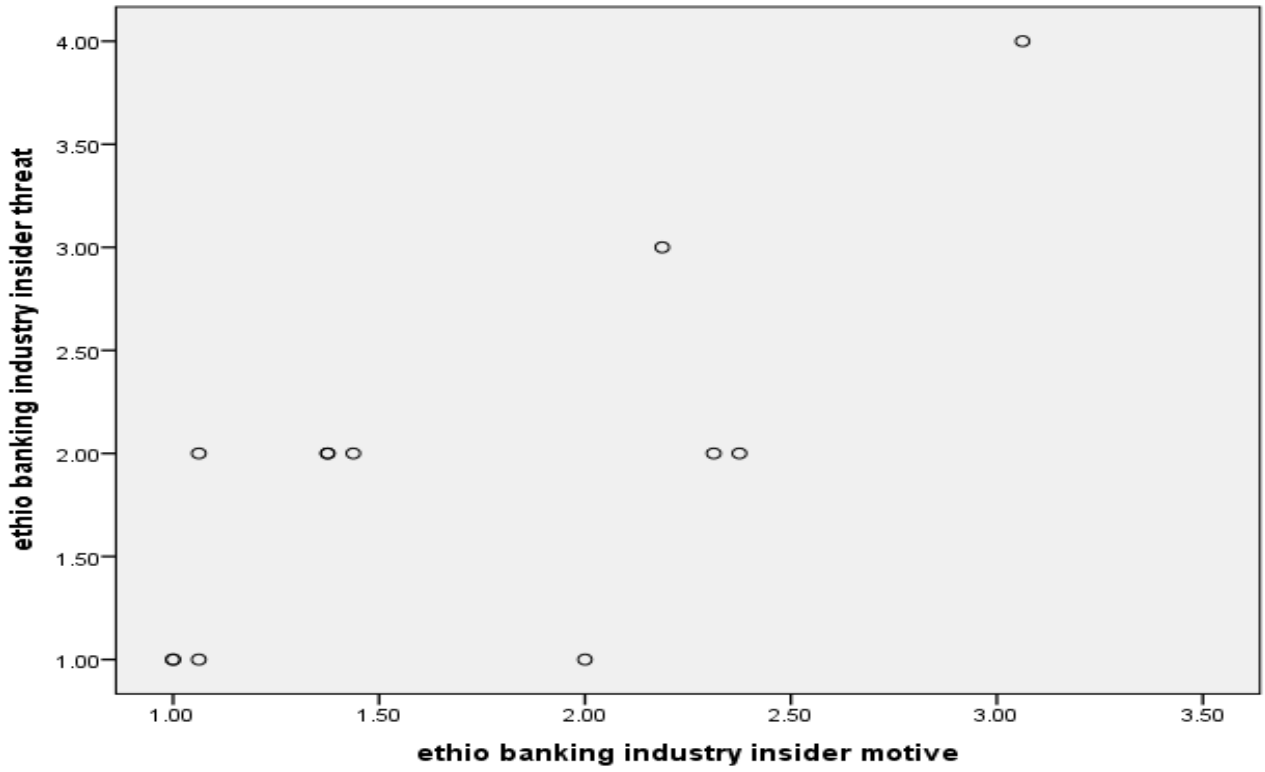


Figure.4.8: The distribution between insider threat and insider motive in Ethiopian banking sector.

From the above distribution chart, the threats and motivation increases in a linear format so the bank should take this in consideration in preparing their insider threat mitigation plan. Each bank should work on those identified motive in advance prior to any incident.

Discussions

The discussion section of this thesis work aimed to utilize the finding from the data analysis to answer the research questions, and then recommend some best practices from the literature reviews.

Discussions Related to Research Question 1
Which insider threats are most prevalent for the Ethiopian commercial banking sector?

The empirical findings showed that the Ethiopian banking sector has experienced various insider incidents in the past with different extent level.

The Installation of unauthorized software threat was ranking the highest as compared to others insider by the participant. There are technological measures that make it difficult for malicious insider users to install unauthorized software on their PC's. These include unified threat management (TMG), block download executable file on the web proxy, and monitoring those users with the help of group policy of the bank at their active directory.

Technological measure is not the only a solution for the problem, it also helps to deal with through policies and disciplinary process. Since some cleaver insiders will always find a way to skirt banks restriction unless they perceive a significant consequence to their action.so every bank should have a software restriction policy in their general information resource policy or bank infrastructure policy. While others such as the financial fraud could be attributed to a combination of poor enforcement of existing information security policies and also poor practices by users.

Due to the implementation of some structural defense mechanisms and using different physical environments controlling mechanisms that are implemented in some of the banks, some of the insider threats are insignificant impact in the business activity of the sectors. Like 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), and Selling employer's confidential information to the competitor are some of the threats that are monitored well by Ethiopian banking sectors.

Discussions Related to Research Question 2

What are the motives behind insider's threats in Ethiopian banking industry?

In many respect, the finding of this study was similar with the finding that has been done by other researchers on financial institutions. In many others research, following financial gain, Revenge is considered to be an important motive for insider. Based on their research, financial gain was considered as one of the greatest motive behind insider threats. The main motives

behind insider threat that this study identified in Ethiopian banking sectors include:

- Dissatisfaction with immediate reporting manager
- Steal data for monetary gain
- Desire for recognition
- Emotional distress(Employee is highly frustrated)

The finding of this study reveals that employees that commit attacks do have different motives. Majority of the motives for carrying out insider threats develop different behavioral changes in accordance to the incidents that occur in their organization. Moreover, it could be analyzed that most of the motives are related to each other. For instance, Emotional distress employee may commit insider threat to take revenge.

Emotional Distress was one of the motives behind insider attack that sometimes forces an individual to commit in Ethiopian Banking sectors. Emotional distress is a state of mind that can occur in an employee due to work pressure or personal problems in its life at any stage. Therefore, banks should follow healthy work culture to utilize productivity of their employees. Emotional distress related with family problem too. Here the HR of a given bank should consider this and related issues that affect the stamina of the employee. Countries like Ethiopia that was in absolute poverty, many people have affected with emotional distress.so special care should be taken during employee recruitment.

All insider attacks have not motives. Threats that happened by accident are conducted by individuals without any motive that happens if an employee is not knowledgeable or does not take organization's security policy casually. Consider a scenario where an employee is about to send a confidential e-mail to his manager. Employee types his manager's mail address incorrectly and sends the mail which is received by another staff member not entitled to read it. This insider incident occurs due to careless attitude of the employee. On the other hand, deliberate threats are planned well in advance and have a motive behind executing an attack.

Discussions Related to Research Question 3

What measures are currently in use to mitigate these insider security threats?

Based on the respondents these mitigation strategies are implemented by most of Ethiopian banking sectors. This includes:

Strict password and account management policies

- Secure physical environment
- Deactivate computer access following termination
- Use of layered defense against remote attacks
- Implementing secure backup and recovery processes
- Tracking and securing of the physical environment (e.g. CCTV systems)
- Use of Data Loss Prevention suites (Restrictions on removal media like flash disks, CDs

There was no single mitigation method which will solve Ethiopian banking sector insider threat problem. So using an integrated mitigation strategy that composes both technical and behavior or psychological method should be implemented. All banks who are currently operating in Ethiopian commercial banking sector recommended sharing some best practices from different financial institute and organization that have a better experience in battling these insider threats.

Strict password and account management policies should be implemented. Access to the bank resources should be granted on need to know basis. In case of change in job role, employee's access rights should be reviewed again to ensure accessibility to only those resources required for the role. Access rights should be granted carefully to ensure that no authorized user is denied access to the resources. Valuable resources should not be accessible to single user alone, instead should be segregated to be accessible in presence of two or more users. Implement secure backup and recovery processes. It is important that organizations prepare for the possibility of an attack or disruption by implementing secure backup and recovery processes that are tested periodically.

Screening of applicants during recruitment should be performed before they join the bank. Checking should be performed in accordance with the details provided in the CV or other information. Checking should be conducted to ensure that employee does not have any criminal background and not involved in activities such as fraud or sabotage in the past. Checking should ensure that employee has never been terminated by the previous employers and has left the company in agreement with the employer.

CHAPTER FIVE

5. Conclusions and Recommendations

5.2. Conclusions

Generally, insiders pose a serious information security threat, costing Ethiopian banking industry millions of Birr in lost revenue. This is a challenging problem to define and study. Insiders cannot be easily profiled and insider attacks are often difficult to detect with incidences. From this study insider threat is not a myth rather a clear threat for Ethiopian commercial banking industry. The findings from the research have shown that the management of insider threat in the context of the commercial banks in Ethiopia needs to be seriously looked at. The critical information assets management in the commercial banks shows that they are vulnerable to insider attacks.

Based on this survey, Installation of unauthorized software and financial fraud should be considered as the main insider threat in the Ethiopian banking sector. So the concerned body should take a responsible measure to reduce the danger that posed by insiders. This could be achieved by monitoring user's computer log and group policy within a specified domain. Others threat such as Social engineering (manipulation of users to obtain formation) and attempt to attach hardware peripherals to desktop systems without authorization had little effect on the information security system of the banks. But this doesn't guarantee for the sustainability of the sector. Early measure should be taken before leading to a catastrophe of higher magnitude.

Most mechanisms currently have employed to enforce more after the fact approaches that are too late into the mitigation. Threat that postured by insider requires preemptive measure. The capable body for the predefined banking ICT security or the ICT division or directorate ought to take care of their data framework security. Implementing different mitigation strategies and creating awareness concerning insiders and other measure must be in place. An employee who was working in information security should have to take advanced training concerning insider threat and information security as a whole.

Finally, by looking instances of insider movement, it is conceivable to find basic examples that show which controls would be best and diminishing the risk. In my understanding an employee can become an insider threat from almost any background or starting point. By understanding insider risk and embracing sensible data security strategies, the danger of both unplanned and malicious threats from insiders can be enormously diminished.

5.1. Recommendations

Combating insider threats is not an easy task. it takes different form. Purely technical approaches seek to specify access control, different monitor devices and other system observables, and harden systems or file structures so as to stop accidental or malicious activities by insiders. Here are some of the recommendations:

- Basic training for all employees should be given about insider and insider threat. Develop ongoing employee awareness, assistance and screening programs.
- Enforce separation of duties and least privilege. Effective separation of duties requires the implementation of least privilege; that is, authorizing people only for the resources they need to do their jobs. Use extra caution with system administrators and privileged users.
- Combating insider threats is not an easy task. It takes different form. Purely technical approaches seek to specify access control, different monitor devices and other system observables, and harden systems or file structures so as to stop accidental or malicious activities by insiders.
- Review the need for individuals who have not undergone appropriate screening to enter or access sensitive areas. Escort or monitor contractors, visitors and others.
- Individual insider activities can be difficult to predict or detect. However, there may be signs that an employee is vulnerable to becoming an insider. Studies reveal a number of indicators to watch for. It is important to note that these are signs of general stress and do not necessarily indicate a propensity to become an insider. They include:

    - ✓ Increased nervousness or anxiety
    - ✓ Decline in work performance
    - ✓ Extreme and persistent interpersonal difficulties

- ✓ Sudden and unexplained wealth
- ✓ Inappropriate interest in sensitive or classified information
- ✓ Accessing (or attempting to access) restricted areas or information outside an employee's realm of responsibility
- ✓ Working unusual hours
- ✓ Unexplained absences or travel

Therefore, it is better to encourage employees to report suspicious behaviour, contacts, enquiries and security breaches.

- Work in the social sciences uses approaches from psychology, organizational behavior, and sociology to delineate insider threat motivations, attempt to predict insider attacks, and change organizational structures and cultures so as to reduce the motivation while better thwarting insider attacks.
- Limit access to files, documents, systems and physical locations to only the individual employees who need this access to undertake their work.
- Consider obtaining legally binding confidentiality undertakings from staff working on potentially sensitive areas or positions. Specially those who are currently working with customer account and related areas, system administrators, etc.

5.3. Suggestion for Future Works.

This work shows the existence of insider threat problem and the current management of insider threat within commercial banking industry in Ethiopia. Most of the respondents (66.6%) said that lack of research on insider threat was one of the challenges that the Ethiopian banking industry currently faces in mitigating the insiders. This kind of research initiatives may lead others researchers to further investigate, predict and prevent malicious insider attacks and other related issues in different organization. Another area of possible future research is to apply the methodology or develop a model that helps to identify and combat insiders within an organization and used to analyze the dynamic nature of the insider threat problem.

References

Aeran (2006).Comprehensive overview of Insider Threats and their Controls. Royal Holloway.

Agata M., Kathryn P. and Marcus B.(2012). Preventing and Profiling Malicious Insider Attacks, Command, Control, Communications and Intelligence Division, Edinburgh South 5111 Australia

Albrechtsen, E., and Hovden, J. 2009. "The Information Security Digital Divide between Information Security Managers and Users," Computers & Security (28:6

Allen, I. E., & Seaman, C. A. (2007). Likert scales and data analyses. Quality Progress, 40(7),64-65.

Association of Certified Fraud Examiner (2008). Report to the Nation on Occupational Fraud and Abuse.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I.(2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly.

Burke, B.E. & Christiansen, C.A.; (2009); Insider Risk Management: A Framework Approach to Internal Security. "RSA, the Security Division of EMC.

C.R. Kothari,(2004), "Research Methodology: Methods and Techniques 2nd",India, New Age International Publishers

Cappelli, D. M., Moore, A. P., Shimeall, T. J., Trzeciak, R. F. (2006).Common Sense Guide to Prevention and Detection of Insider Threats, Version 2.1, Carnegie Mellon University/CyLab.

Cappelli, D. M., Moore, A. P., Trzeciak, R. F., Shimeall, T. J. (2009).Common Sense Guide to Prevention and Detection of Insider Threats, Version 3.1, Carnegie Mellon University/Cy Lab.

Centre for the Protection of National Infrastructure (CPNI) (United Kingdom). (2014). CPNI Insider Data Collection Study: report of main findings

Colwill, C. (2010). Human factors in information security: The insider threat- Who can you trust these days? Information Security Technical Report, 14, 186-196.

Connelly,.L.m.(2008).pilot studies.medsurg Nursing,17(6),411-2

CSO magazine, USSS, CERT, and Deloitte. (2011, 12 March 2013). 2011 Cyber security Watch Survey: Organizations need more skilled cyber professionals to stay secure.

D.F. Ferraiolo, D.R. Kuhn, R. Chandramouli, (2003). Role Based Access Control, Artech House.

Dhillon, G. & Torkzadeh (2006). Value-focused assessment of information system security in organizations. Information Systems Journal, 16, 293-314.[37]

Dlamini, M.T., Eloff, J.H.P., and Eloff, M.M. (2009). "Information Security: The Moving Target," 38 Computers & Security (28:3-4), pp. 189-198.

Dwight Allison, (2012).The insider threat problem: the case of a Jamaican government organization. Lulea University of technology

E. Bertino, P. A. Bonatti and E. Ferrari. (2001). A temporal role-based access control. ACM Transactions on Information and System Security, 4(3), pages 191- 223

Esola, L. (2007). Employee fraud is key concern for financial institutions. Business Insurance, 41(35), 11-12. Employee fraud, Information Systems Journal, 22(2), 30-38.

Fischer, L.F. (2008). Espionage: Why does it happen? Retrieved June 2009,

Gartner (2008). "Best Practices for Managing 'Insider' Security Threats,"

Goddard, W & Melville, S. (2004). Research Methodology: An Introduction. Lansdowne: Juta and Company Ltd.

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

Halefom Hailu, (2014). The state of cybercrime governance in Ethiopia

Holmlund, L., Mucisko, D., Lynch, R., & Freyre, J. (2011). 2011 Cyber Security Watch Survey: Organizations Need More Skilled Cyber Professionals To Stay Secure: CERT Program, Software Engineering Institute, Cargegie Mellon.

Intelligence and National Security Alliance (2013), preliminary examination Of insider threat programs in the U.S. private sector.

ISO/IEC 27001:2005. Information technology Security techniques – Information security management systems – Requirements.

ISO/IEC, Information technology Security techniques-Information security risk management" ISO/IEC FIDIS 27005:2008

Jon Oltsik, (2013), Vormetric / ESG Insider Threats Survey threat: The Ominous State of Insider Threats

Joseph S., Jeffrey L., Jay F., Salim H.,(2013). "Identifying Insider threats through monitoring mouse movements in concealed information tests." Proceedings of the HICSS-46 symposium on credibility assessment and information quality in government and business.

Josephine W. (2012). Combating Insider Threat Using Behaviour Based Access Control.

K. Nance and R. Marty,(2011)."Identifying and visualizing the malicious insider threat using bipartite graphs," in 44th Hawaii International Conference on System Sciences (HICSS), Koloa, Kauai, Hawaii, USA, 2011, pp. 1-9.

Kelemie T. (2013), Information security management framework for banking industry in Ethiopia

Kirlappos, I Beautement, A., and Sasse, M. A. (2013),. "'Comply or Die' Is Dead: Long Live Security-Aware Principal Agents The Need for Information Security," in Financial Cryptography and Data Security, Springer Berlin Heidelberg, pp. 70–82.

Kombo, D. K & Tromp, D. L. A. (2006) Proposal and Thesis Writing: An Introduction.Daughters of St. Paul. Paulines Publications Africa.

Kowalski, E.F., Cappelli, D.M., and Moore, A.P. 2008. Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector. Joint SEI and U.S. Secret Service Report, January 2008.

Lemma Lessa and Abiy Woretaw, (2012).Information security culture in the banking sector in Ethiopia

Liu, S. & B. Cheng. (2009). Cyber attacks: Why, what, who, and how, IT Pro, May/June 2009.

Martinez-Moyano, I. J. et al. (2008). A Behavioral Theory of Insider-Threat Risks: A System Dynamics Approach. ACM Transactions on Modeling and Computer Simulations 18 (2), pp. 7-34.

Martinez-Moyano, I., E. Rich, S. Conrad, D. Andersen, and T. Stewart. (2008). Abehavioural theory of insider threat risks: a system dynamics approach. ACM Transactions on Modelling and Computer Simulation.

Melara, C. et al. (2003). A System Dynamics Model of an Insider Attack on an Information System.In Proceedings of the 21st International Conference of the System Dynamics Society (New York, USA, July 20-24).

Michael E. Whitman and Herbert J. Mattord (2008).Principles of Information Security, Thomson Course Technology.

Michael E. Whitman and Herbert J. Mattord (2008).Principles of Information Security, Thomson Course Technology.

Montelibano and Andrew Moore, (2012) TECHNICAL REPORT CMU/SEI-2012-TR-007 ESC-TR-2012-007 CERT® Program 14. Smith, A. D. (2005). Accountability in EDI systems to prevent

Montelibano,J. & Moore, A.;(2012): "Insider Threat Security Reference Architecture." TECHNICAL REPORT - CERT Program

Moore, A.P., Cappelli, D.M., & Trzeciak, R.F. (2008).The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructure. CERT Technical Report, CMU/SEI-2008-TR-009, May 2008.

Munshi, Asmaa, Peter Dell, and Helen Armstrong(2012) "Insider threat behavior factors: A comparison of theory with reported incidents." System Science (HICSS), 2012 45th Hawaii International Conference on. IEEE

NBE (1963). Proclamation No. 206/1963: A Proclamation to Provide for the Regulation of the Monetary and Banking System, Addis Ababa.

NBE (1994). Proclamation No. 83/1994: Monetary and Banking Proclamation, Addis Ababa.

NBE (1996.Directive No. SBB/12/1996: Limitation on Investment of Banks, Licensing and supervision of Banking business, Addis Ababa.

NBE (1999).Directive No. SBB/24/1999: Minimum Paid up Capital to be Maintained by Banks", Licensing and supervision of Banking business, Addis Ababa.

Porter, D. (2003). Insider Fraud: Spotting The Wolf In Sheep's Clothing. Computer Fraud and Security, 4, 12-15.

PricewaterhouseCoopers UK,2013.Randazzo, M., Keeney, M., Kowalski, E., Capelli, D., and Moore, A., (2004), Insider threat study: illicit cyber activity in the banking and finance sector, N.T.A.C. U.S. Secret Service and CERT Coordination Centre, S.E.I., Carnegie Mellon University, August 2004

PwC (2012) Information Security Breaches Survey: Technical report, information security-breaches-survey-technical-report.pdf

PwC. (2014) "Key findings from The Global State of Information Security ® Survey 2014," .

R. Chinchani, A. Iyer, H. Q. Ngo, and S. Upadhyaya, "Towards a theory of insider threat assessment," in International Conference on Dependable Systems and Networks, Yokohama, Japan, 2005, pp. 108-117.

R. Richardson,(2007). computer crime and security survey," Computer Security Institute,

Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A., (2005). Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector. U.S. Secret Service and CERT Coordination Centre: Software Engineering Institute.

Redman, L. V & Mory, A. V. H. (2009).The Romance of Research. Baltimore: The Williams & Wilkins Co.

Rob Johns,(2010) .Likert items and scales: survey question bank: Methods Fact Sheet 1 (March 2010)

Ronald Jay P, (2005). Essentials of survey research and analysis

Ronald Jay P., (2005) .Essentials of survey research and analysis

Roy Sarkar, K. (2010). Assessing insider threats to information security using technical, behavioral and organisational measures.Information Security Technical Report

S. Pramanik, V. Sankaranarayanan, and S. Upadhyaya,(2009). "Security policies to mitigate insider threat in the document control domain," Tucson, Arizona, USA. IEEE,

Schneier, B. (2004). "Secrets & lies, digital security in a networked world." Wiley Publishing

Sekaran, U. (2003). Research methods for business: A skill building approaches (4th ed.). New York: John Wiley & Sons, Inc.

Shaw, E.D., Ruby, K.G., & Post, J. M. (1998).The insider threat to information systems. Security Awareness Bulletin, 2–98, 27–46.

Silo wash, G., Cappelli, D. Moore, A., Trzeciak, R., Shimeall, T. J. and Flynn, L.; (2012); Common Sense Guide to Mitigating Insider Threats 4th Edition

Silowash, George; Cappelli, Dawn; Moore, Andrew; Trzeciak, Randall; Shimeall, Timothy; & Flynn, Lori, (2012).*Common Sense Guide to Mitigating Insider Threats, 4th Edition* (CMU/SEI-2012-TR-012).Software Engineering Institute, Carnegie Mellon University, 2012.

Simeneh T.(2013). Prospects and challenges of private commercial banks in Ethiopia December,

Siponen, M., Mahmood, M. A., & Pahnila, S. (2009). Are Employees Putting Your Company at Risk by Not Following Information Security Policies? Communications of the ACM, 52(12), 145-147.

Software Engineering Institute. (2011) Cyber Security Watch Survey. Software Engineering Institute, Carnegie Mellon University.

Tang, G. L.(2005). Trusted computing: addressing insider threats to the banking and financial sector.

Tang, Gene L. (2005), Trusted computing: addressing insider threats to the banking and financial sector.

Tekle Beirhan G (2008). "Financial Sector Development in Ethiopia: Trend and Risks", in Birritu special publication N0.100, Addis Ababa.

Terry Chia (2013), Confidentiality, Integrity, Availability: The three components of the CIA Triad

The 2015 Vormetric Insider Threat Report, Trends and Future Directions in Data Security Global Edition,

US Secret Service and Carnegie Mellon University Software Engineering Institute CERT. (2008).Insider Threat Study: Illicit Cyber Activity in the Government Sector.

US Secret Service and CERT Coordination Centre, Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector, August 2004,

Verizon. (2013).Data Breach Investigations Report," .

Willison, R., and Warkentin, M. (2013). "Beyond Deterrence: An Expanded View of Employee Computer Abuse," MIS Quarterly (37:1), pp.1–20

Yegidis, B. L. &Weinbach, R. W. (1996), Research Methods for Social Workers, 2nd. Edition, Allyn and Bacon, Boston, Massachusetts

Zerayehu S., Kagnew W., Teshome K.,(2013). Competition in Ethiopian Banking Industry, University of Nairobi, Kenya.

Zhou, C. V., Leckie, C., & Karunasekera, S. (2010). A survey of coordinated attacks and collaborative intrusion detection. Computers and Security, 29(1), 124–140.

Web sites (URLs)

www.vormetric.com/InsiderThreat/2015.

The World Bank, http://data.worldbank.org/country/ethiopia

http://www.hanford.gov/oci/maindocs/ci_r_docs/whyhappens.pdf

CERT Insider threat site. http://www.cert.org/insider_threat

| www.insaonline.org

Appendix A

Research Questionnaire

The following questionnaire will require approximately Ten min to complete. In order to ensure that all information will remain confidential, please do not include your name. Be assured that any information provided will be treated in confidence and none of the participants will be individually identifiable in the resulting report. If you require additional information or have questions, please contact me at the number listed below.

Thank you for taking the time to assist me in my educational endeavors.

Part I: DEMOGRAPHIC INFORMATION

1. Please mark (X) to indicate your Gender?

( ) Male ( ) Female

2. Please mark (X) to indicate your age?

( ) Below 25
( ) Between 25 and 30
( ) Between 31 and 35
( ) Between 36 and 40
( ) Between 41 and 45
( ) 46 and Above

3. What is your role/position inside your Bank?

( ) Director
( ) IT manager
( ) Chief Information Officer
( ) Senior Network Administrator
( ) Senior System Administrator
( ) MIS Officer
( ) Others (Specify) _____

4. How many years of experience do you have in this role in the bank?

- ( ) Below 5 Years
- ( ) Between 6 and 10 Years
- ( ) Between 11 and 15 Years
- ( ) Between 16 and 20 Years
- ( ) Over 20

5. The number of employees in your bank?

- ( ) Below 50
- ( ) Between 51 and 500
- ( ) Between 501 and 1000
- ( ) Between 1000 and 5000
- ( ) Above 5000

6. The number of branches owned by your bank?

- ( ) Below 10
- ( ) Between 11 and 30
- ( ) Between 31 and 50
- ( ) Between 51 and 70
- ( ) Between 71 and 100
- ( ) Above 100

7. What is the average age in years of the perpetrators of insider threats encountered in your bank? (this only if you have a case related to fraud caused by insiders)

- ( ) Below 25

( ) Between 25 and 30

( ) Between 31 and 35

( ) Between 36 and 40

( ) Between 41 and 45

( ) 46 and Above

8. What is percentage of the central IT budget would you estimate spent on information security?

( ) Less than 1%

( ) Between 1 and 5%

( ) Between 5 and 10%

( ) Between 10 and 15%

( ) Greater than 15%

Part II: INSIDER THREATS

9. Please mark (X) 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
Destruction of critical data					
Theft of critical information like bank customers records and business plan					
Financial fraud					
Spoofing(pretending to be something or someone that one is not)					
Computer virus implantation					
Social engineering (manipulation of users to obtain formation)					
Installation of unauthorized software					
Purposefully installing malicious software					
Impersonation of other users					
Sabotage (disrupting operations, network)					
Tampering with data (unauthorized changes of data or records)					
Unauthorized Access					
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)					

Malicious programs or Trojan horse programs were installed on company assets					
Attempt to attach hardware peripherals to desktop systems without authorization					
Others (Specify and Rate accordingly)					

10. 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**
Negligent Insiders - Insiders who accidentally expose data – such as an employee who forgets their laptop on an airplane					
Malicious Insiders - Insiders who intentionally steal data or destroy systems – such as a disgruntled employee who deletes some records on his last day of work					
Compromised Insiders - Insiders whose access credentials or computers have been compromised by an outside attacker					
Others(Specify and Rate accordingly)					

11. Please mark (X) to indicate the extent to which perpetrators of insider threats in your bank have or have exhibited/displayed the following **b**ehavioral element or characteristics?

12. Please mark (X) to indicate the extent to which the following motivations could have been the driving force behind the insider threats experienced in your bank?

Behaviors or Characteristics Displayed	**No Extent at All**	**Little Extent**	**Moderate**	**Great Extent**	**Very Great Extent**
Remotely accesses the network while on vacation, sick or at odd times					
Uncharacteristic comments made to co-workers					
Unnecessarily copies material, especially if it is proprietary or classified					
Drop in performance and/or attendance					
Interest in matters outside of the scope of their duties					
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 preoccupied)					
Imitation and modeling those whom they respect					
Others (Specify and Rate accordingly)					

Motivation	No Extent at All	Little Extent	Moderate Extent	Great Extent	Very Great Extent
Steal data for monetary gain (stealing or manipulating financial details for personal monetary benefits)					
Disrupt critical systems for ideological reasons					
Dissatisfaction with bank's policies					
Dissatisfaction with immediate reporting manager					
Desire for recognition					
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)					
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's network resulting in disruption of services)					
Hooliganism(such as defacing a Web site)					
Family problems					
Challenge security professionals					
Others (Specify and Rate accordingly)					

Part III: **MITIGATION**

13. 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
Develop an insider incident response plan					
Periodic security awareness training for all employees					
Separation of duties and least privilege					
Strict password and account management policies					
Secure physical environment					
Deactivate computer access following termination					
Consider threats from insiders and business partners in enterprise-wide risk assessment					
Contracted service organizations or third party agree to abide by designated security and confidentiality policies.					
Use of layered defence against remote attacks					
Log, monitor and audit employee online actions					
Use of extra caution with privileged users					
Anticipate and manage negative workplace issues					
Consider secure coding in SDLC					
Implement system change controls removal.					
Implementing secure backup and recovery processes					
SIEM or other log analysis					
Monitor and respond to suspicious or disruptive behavior					
Tracking and securing of the physical environment (e.g. CCTV					

systems)					
Use of Data Loss Prevention suites (Restrictions on removal media like flash disks, CDs, etc.)					
Stringent Service Level Agreements with third party service providers					
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 behaviors from their colleagues					
Work together across the Bank(increase all staff participation)					
Others (Specify and Rate accordingly)					

14. What major challenges the bank has experienced in prevention and implementation of insider threats mitigation strategies?

Challenges in Prevention	No Extent at All	Little Extent	Moderate Extent	Great Extent	Very Great Extent
Lack of research on insider threat					
Lack of education and awareness about insider threats					
Unavailability to specific technology solutions					
Lack of technical experience in using security tools					
Lack of Suitable Legal and Regulatory Framework in regulating insiders threats.					
Vendor/Contractor management Issues					
Lack of information sharing					
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 B

የኢትዮጵያ ብሔራዊ ባንክ
National Bank of Ethiopia

Annex I

Actual or Attempted Fraud Cases

Name of bank: _____
Date: _____

No.	Items	Description	Remark
1.	Name and complete address of the suspected fraudster		
2.	Description or type of fraud (embezzlement, cheating, forgery using fake instruments or others)		
3.	Causes of the fraud		
4.	Status or profession of the suspected fraudster (director, employee, customer, or other party)		
5.	Amount of actual or estimated fraud		
6.	Date of occurrence of fraud		
7.	Date of detection of fraud and reason for the delay to detect (if any)		
8.	Place and area of operation where the fraud has occurred		
9.	Technique and/or technology used to commit the fraud		
10.	Action taken or proposed to be taken to avoid such incidents		
11.	Amount recovered, if any		
12.	In case of attempted fraud, state reason for the failure of the fraud action		
13.	Any other relevant information		

Prepared by: _____
Signature: _____
Date: _____

Approved by: _____
Signature: _____
Date: _____

4

Appendix C

SPSS outputs

Frequency Table for insider threat

The Std. Deviation was computed here.

Statistics

		Destruction of critical data	Theft of critical information like bank customers records and business plan	Financial fraud	Spoofing(pretending to be something or someone that one is not)
N	Valid	16	17	16	18
	Missing	2	1	2	0
Mean		1.5625	1.8824	2.3125	1.7778
Mode		1.00	1.00	2.00	1.00
Std. Deviation		.72744	1.05370	1.01448	1.11437
Percentiles	25	1.0000	1.0000	2.0000	1.0000
	50	1.0000	2.0000	2.0000	1.0000
	75	2.0000	2.5000	2.7500	2.0000
	100	3.0000	4.0000	5.0000	4.0000

Statistics

		Computer virus implantation	Social engineering (manipulation of users to obtain formation)	Installation of unauthorized software	Hacking(accesses a computer system by circumventing its security system)
N	Valid	17	18	18	18
	Missing	1	0	0	0
Mean		2.0000	2.0556	3.0000	1.4444
Mode		1.00	1.00	2.00	1.00
Std. Deviation		1.17260	1.16175	1.23669	.61570
Percentiles	25	1.0000	1.0000	2.0000	1.0000
	50	2.0000	2.0000	3.0000	1.0000
	75	2.5000	3.0000	4.0000	2.0000
	100	5.0000	5.0000	5.0000	3.0000

Statistics

		Purposefully installing malicious software	Impersonation of other users	Sabotage (disrupting operations, network)	Tampering with data (unauthorized changes of data or records)
N	Valid	18	18	18	18
	Missing	0	0	0	0
Mean		1.3333	1.6667	1.7222	1.8889
Mode		1.00	2.00	1.00	2.00
Std. Deviation		.68599	.76696	.89479	.96338
Percentiles	25	1.0000	1.0000	1.0000	1.0000
	50	1.0000	2.0000	1.5000	2.0000
	75	1.2500	2.0000	2.0000	2.0000
	100	3.0000	4.0000	4.0000	4.0000

Statistics

		Unauthorized Access	Denial of service attacks	Organized Crime(Insiders colluding with criminal gangs)	Identity Thieves(Impersonation Fraudsters)
N	Valid	18	18	18	18
	Missing	0	0	0	0
Mean		1.7778	1.2778	1.3333	1.5000
Mode		1.00	1.00	1.00	1.00
Std. Deviation		1.16597	.57451	.59409	.78591
Percentiles	25	1.0000	1.0000	1.0000	1.0000
	50	1.0000	1.0000	1.0000	1.0000
	75	2.0000	1.2500	2.0000	2.0000
	100	5.0000	3.0000	3.0000	4.0000

Statistics

		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)
N	Valid	18	17	18	18
	Missing	0	1	0	0
Mean		1.2222	1.7059	1.6111	1.3889
Mode		1.00	1.00	1.00	1.00
Std. Deviation		.42779	.84887	.69780	.60768
Percentiles	25	1.0000	1.0000	1.0000	1.0000
	50	1.0000	2.0000	1.5000	1.0000
	75	1.2500	2.0000	2.0000	2.0000
	100	2.0000	4.0000	3.0000	3.0000

Statistics

		Selling employer's confidential information to the competitor(s)	Malicious programs or Trojan horse programs were installed on company assets	Attempt to attach hardware peripherals to desktop systems without authorisation
N	Valid	18	18	18
	Missing	0	0	0
Mean		1.5000	2.0556	1.9444
Mode		1.00	2.00	1.00
Std. Deviation		.85749	.87260	1.16175
Percentiles	25	1.0000	1.0000	1.0000
	50	1.0000	2.0000	2.0000
	75	2.0000	3.0000	2.2500
	100	3.0000	4.0000	5.0000

a. Multiple modes exist. The smallest value is shown

Correlations

		ethio banking industry insider threat	ethio banking industry insider challenge	ethio banking industry insider motive	ethio banking industry mitgation
ethio banking industry insider threat	Pearson Correlation	1	.707*	.733**	.211
	Sig. (2-tailed)		.010	.007	.585
	N	14	12	12	9
ethio banking industry insider challenge	Pearson Correlation	.707*	1	.597*	-.148
	Sig. (2-tailed)	.010		.040	.665
	N	12	14	12	11
ethio banking industry insider motive	Pearson Correlation	.733**	.597*	1	.243
	Sig. (2-tailed)	.007	.040		.472
	N	12	12	15	11
ethio banking industry mitgation	Pearson Correlation	.211	-.148	.243	1
	Sig. (2-tailed)	.585	.665	.472	
	N	9	11	11	12

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

		Steal data for monetary gain (stealing or manipulating financial details for personal monetary benefits	Disrupt critical systems for ideological reasons	Dissatisfaction with bank's policies	Dissatisfaction with immediate reporting manager
N	Valid	17	18	16	18
	Missing	1	0	2	0
Mean		2.1765	1.3333	1.8125	1.8889
Mode		1.00	1.00	1.00	1.00[a]
Std. Deviation		1.23669	.84017	1.16726	.90025
Percentiles	25	1.0000	1.0000	1.0000	1.0000
	50	2.0000	1.0000	1.0000	2.0000
	75	3.5000	1.0000	2.0000	2.2500
	100	4.0000	4.0000	4.0000	4.0000

Statistics

		Desire for recognition	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)
N	Valid	18	18	18	18
	Missing	0	0	0	0
Mean		2.2222	1.6667	1.4444	1.7222
Mode		2.00	1.00	1.00	1.00[a]
Std. Deviation		1.00326	.97014	.61570	.95828
Percentiles	25	1.0000	1.0000	1.0000	1.0000
	50	2.0000	1.0000	1.0000	1.0000
	75	3.0000	2.0000	2.0000	2.2500
	100	4.0000	4.0000	3.0000	4.0000

Statistics

		Revenge (employees with negative feelings towards the company or individuals within the company)	Emotional distress(Employee is highly frustrated)	Sabotage (disruption of company operations)	Theft (data stored in computer hardware and software, company or customer financial data)
N	Valid	18	17	18	18
	Missing	0	1	0	0
Mean		1.7222	1.8824	1.3889	1.3889
Mode		1.00	1.00	1.00	1.00[a]
Std. Deviation		1.12749	1.05370	.69780	.60768
Percentiles	25	1.0000	1.0000	1.0000	1.0000
	50	1.0000	2.0000	1.0000	1.0000
	75	2.0000	2.5000	2.0000	2.0000
	100	5.0000	4.0000	3.0000	3.0000

Statistics

		Curiosity (experimenting with company's network resulting in disruption of services)	Hooliganism(such as defacing a Web site)	Family problems	Challenge security professionals
N	Valid	18	18	18	18
	Missing	0	0	0	0
Mean		1.5000	1.4444	1.7222	1.7222
Mode		1.00	1.00	1.00	1.00[a]
Std. Deviation		.70711	.61570	.95828	1.01782
Percentiles	25	1.0000	1.0000	1.0000	1.0000
	50	1.0000	1.0000	1.0000	1.0000
	75	2.0000	2.0000	2.2500	2.0000
	100	3.0000	3.0000	4.0000	4.0000

a. Multiple modes exist. The smallest value is shown

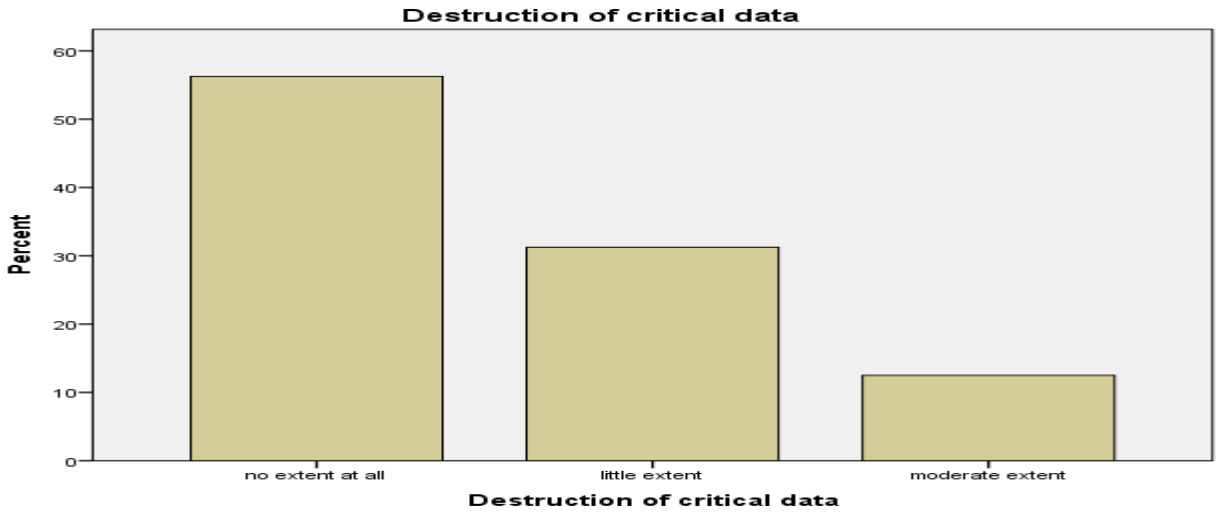
```
COMPUTE NEWTREAT=insider_threat_1 + insider_threat_2 +  insider_threat_3 +
insider_threat_4 + insider_threat_5 + insider_threat_6 + insider_threat_7 +
insider_threat_8 + insider_threat_9 + insider_threat_10 + insider_threat_11
+ insider_threat_12 +
insider_threat_13 + insider_threat_14 + insider_threat_15 +
insider_threat_16 + insider_threat_17 + insider_threat_18 +
insider_threat_19 + insider_threat_20 + insider_threat_21 +
insider_threat_22 + insider_threat_23.
EXECUTE.
COMPUTE NEWTYPE=type_of_in_1 + type_of_in_2 + type_of_in_3 .
EXECUTE.
COMPUTE NEWBEHR=behavior_1 + behavior_2 + behavior_3 + behavior_4 +
behavior_5 + behavior_6 + behavior_7 + behavior_8 + behavior_9 +
behavior_10 + behavior_11 + behavior_12 + behavior_13 + behavior_14 +
behavior_15 + behavior_16 + behavior_17 +
behavior_18 + behavior_19 + behavior_20 + behavior_21 + behavior_22 +
behavior_23.
EXECUTE.
COMPUTE NEWMOTIVATION=motivation_1 + motivation_2 + motivation_3 +
motivation_4 + motivation_5 + motivation_6 + motivation_7 + motivation_8 +
motivation_9 + motivation_10 + motivation_11 + motivation_12 +
motivation_13 + motivation_14 + motivation_15 +
motivation_16 .
EXECUTE.
COMPUTE NEWMITIGATION=mitigation_1 + mitigation_2 + mitigation_3 +
mitigation_4 + mitigation_5 + mitigation_6 + mitigation_7 + mitigation_8 +
mitigation_9 + mitigation_10 + mitigation_11 + mitigation_12 +
mitigation_13 + mitigation_14 + mitigation_15 +
```

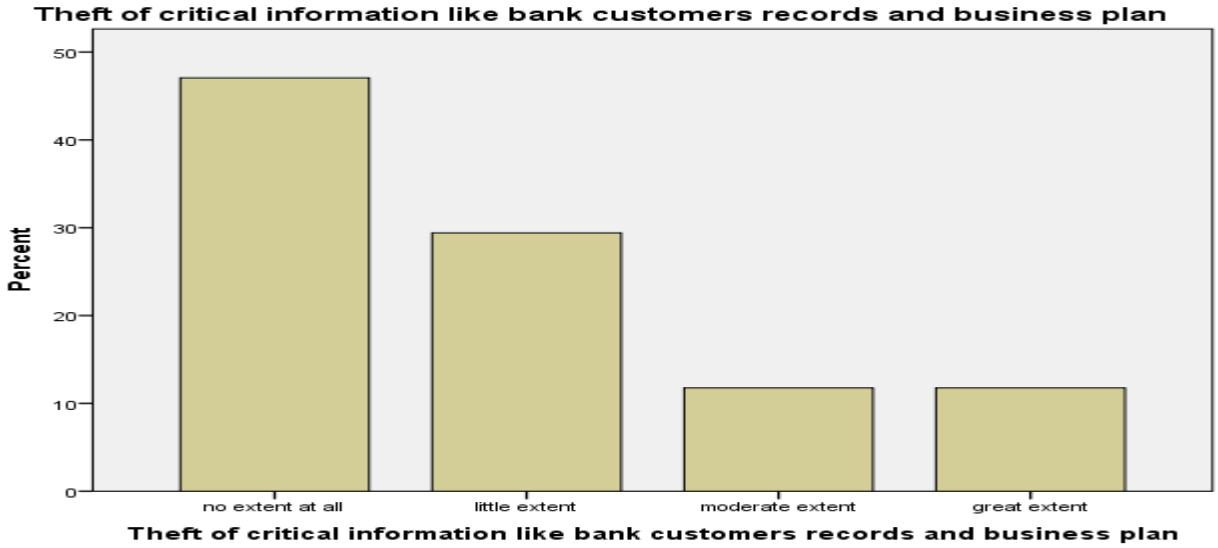
```
mitigation_16 + mitigation_17 + mitigation_18 + mitigation_19 +
mitigation_20 + mitigation_21 + mitigation_22 + mitigation_23 +
mitigation_24 + mitigation_25.
EXECUTE.
COMPUTE NEWCHALLEGE=challenge_1 + challenge_2 + challenge_3 + challenge_4 +
challenge_5 + challenge_6 + challenge_7 + challenge_8 + challenge_9 +
challenge_10 + challenge_11 + challenge_12 + challenge_13 .
EXECUTE.
COMPUTE ethio banking industry insider threat =NEWTREAT / 23.
EXECUTE.
COMPUTE newisider1=NEWTYPE / 3.
EXECUTE.
COMPUTE newbevhr=NEWBEHR / 23.
EXECUTE.
COMPUTEethio banking industry insider motive =NEWMOTIVATION / 16.
EXECUTE.
COMPUTE ethio banking industry mitigation =NEWMITIGATION / 25.
EXECUTE.
COMPUTE ethio banking industry insider challenge =NEWCHALLEGE / 13.
EXECUTE.
CORRELATIONS
  /VARIABLES=newtreat1 newisider1
  /PRINT=TWOTAIL NOSIG
  /MISSING=PAIRWISE.
```

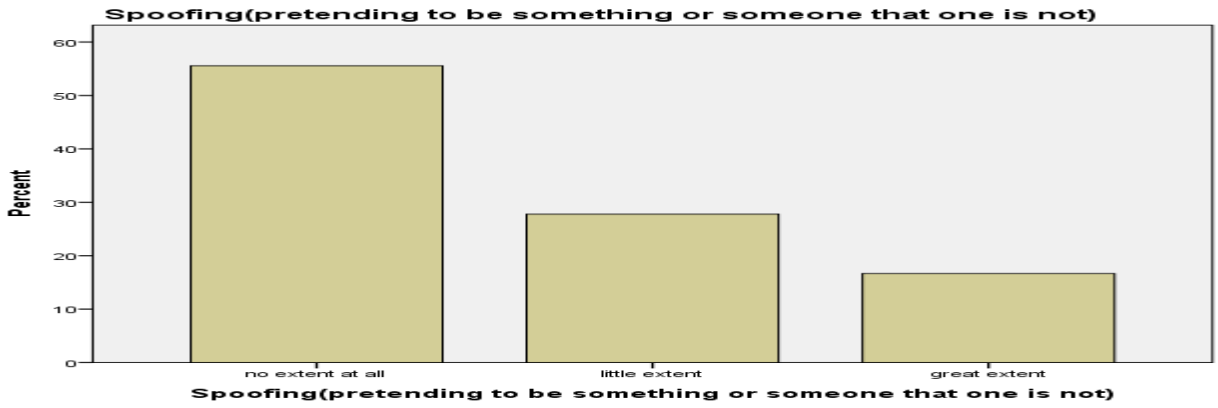
Installation of unauthorized software

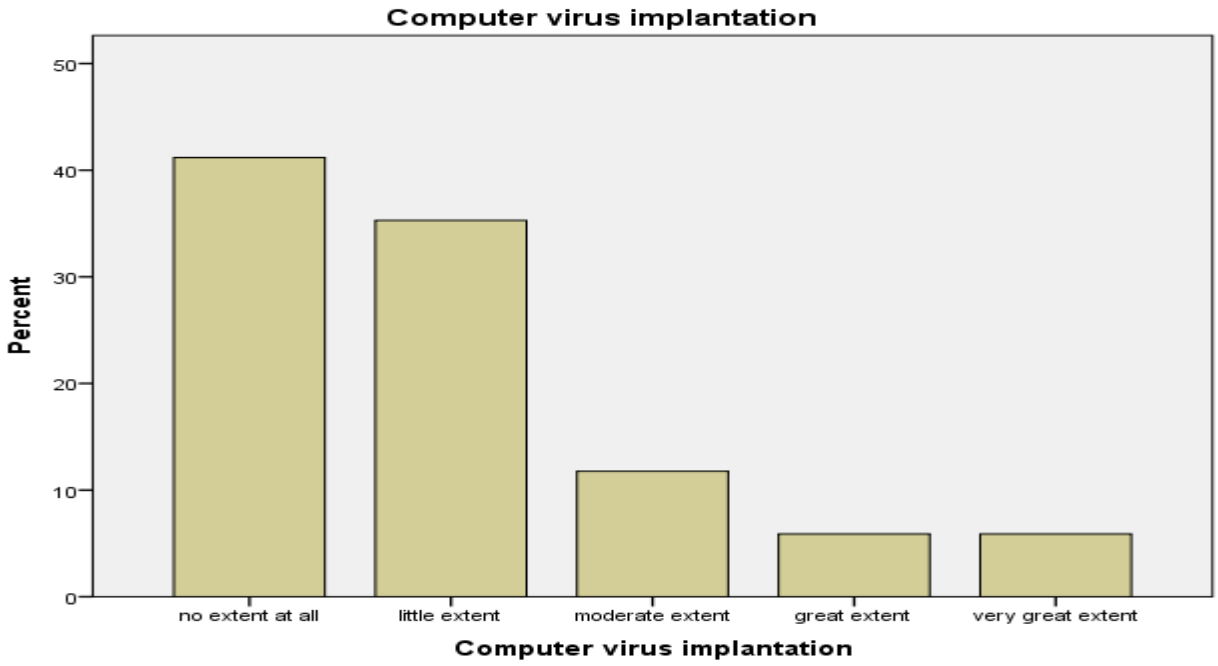
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no extent at all	2	11.1	11.1	11.1
	little extent	5	27.8	27.8	38.9
	moderate extent	4	22.2	22.2	61.1
	great extent	5	27.8	27.8	88.9
	very great extent	2	11.1	11.1	100.0
	Total	18	100.0	100.0	

Bar Chart


Destruction of critical data
Percent
60
50
40
30
20
10
0
no extent at all
little extent
moderate extent
Destruction of critical data


Theft of critical information like bank customers records and business plan
Percent
50
40
30
20
10
0
no extent at all
little extent
moderate extent
great extent
Theft of critical information like bank customers records and business plan


Spoofing(pretending to be something or someone that one is not)
Percent
60
50
40
30
20
10
0
no extent at all
little extent
great extent
Spoofing(pretending to be something or someone that one is not)


Computer virus implantation
Percent
50
40
30
20
10
0
no extent at all
little extent
moderate extent
great extent
very great extent
Computer virus implantation

Appendix D

List of commercials Banks currently operating in Ethiopia

1. Commercial Bank of Ethiopia
2. Development Bank of Ethiopia
3. Construction and Business Bank of Ethiopia
4. Debube Global Bank
5. Wegagen bank
6. United Bank
7. Buna International Bank
8. Berhan Bank
9. Abaye Bank
10. Addis International Bank
11. Awash International Bank
12. Cooperative Bank of Oromia
13. Oromia International Bank
14. Nib International bank
15. Lion International Bank
16. Abyssinia Bank
17. Zemen Bank
18. Enat Bank
19. Dashen Bank

Declaration

I declare that the thesis is my original work and has not been presented for a degree in any other university.

_____

Behabtu Amare

June 2015

This thesis has been submitted for examination with my approval as university advisor.

_____

Advisor's Name Signature

Date _____