

**AN UPDATE TO THE INSIDER SYSTEM SECURITY ATTACK PREDICTION  
MODEL TO SUIT SELECTED PUBLIC UNIVERSITIES IN KENYA**

**Wapukha Walumbe Denis**

**(Bsc. Computer Science Masinde Muliro University)**

**A Thesis Submitted to the School of Post Graduate Studies in Partial Fulfilment of  
the Requirement for the Award of Degree of Master of Science in Information  
Systems In School of Information Science and Technology, Kisii University**

**November, 2020**

## DECLARATION

This thesis is my original work and has not been presented elsewhere for a degree on any other university.

### Student Name

**Walumbe Wapukh Denis**    Signature.....    Date...../...../.....  
**MIN11/20403/14**

## DECLARATION BY THE SUPERVISOR

The thesis has been submitted for examination with our approval as University supervisors.

**Dr. Jame Ogalo**                      Signature.....    Date...../...../.....

Lecturer of Computing and Science  
Kisii University

**Dr. Wasike Jotham**                      Signature.....    Date...../...../.....

Lecturer, Communication and Information Technology  
Kirinyaga University

# DECLARATION OF PLAGIARISM

KSU/SPGS/PG/03

Telephone : +254 710 886467  
Email : spgs@kisiiuniversity.ac.ke



P. O. Box 408-40200  
KISII, KENYA  
www.kisiiuniversity.ac.ke

## KISII UNIVERSITY OFFICE OF THE DIRECTOR POST GRADUTATE STUDIES

### PLAGIARISM DECLARATION

#### **Definition of plagiarism**

*Is academic dishonesty which involves; taking and using the thoughts, writings, and inventions of another person as one's own.*

#### **DECLARATION BY STUDENT**

- i. I declare I have read and understood Kisii University rules and regulations, and other documents concerning academic dishonesty
- ii. I do understand that ignorance of these rules and regulations is not an excuse for a violation of the said rules.
- iii. If I have any questions or doubts, I realize that it is my responsibility to keep seeking an answer until I understand.
- iv. I understand I must do my own work.
- v. I also understand that if I commit any act of academic dishonesty like plagiarism, my thesis/project can be assigned a fail grade ("F")
- vi. I further understand I may be suspended or expelled from the University for Academic Dishonesty.

Name WALUMBE W. DENIS

Signature [Signature]

Reg. No M/PH/1/2018/03/2020

Date 01/10/2020

#### **DECLARATION BY SUPERVISOR (S)**

- i. I/we declare that this thesis/project has been submitted to plagiarism detection service.
- ii. **The thesis/project contains less than 20% of plagiarized work.**
- iii. I/we hereby give consent for marking.

1. Name \_\_\_\_\_

Signature \_\_\_\_\_

Affiliation \_\_\_\_\_

Date \_\_\_\_\_

2. Name Dr. Jotham Wasike

Signature [Signature]

Affiliation Kinnyaga University

Date 6/10/2020

3. Name \_\_\_\_\_

Signature \_\_\_\_\_

Affiliation \_\_\_\_\_

Date \_\_\_\_\_

*Our vision: A world class University and advancement of education, excellence research & social welfare.*

UNIVERSITY IS ISO 9001:2008 CERTIFIED



## **COPYRIGHT**

All rights are reserved. No part of this **thesis or information herein** may be reproduced, stored in a retrieval system or transmitted in any form or by any means electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the author or Kisii University on that behalf.

**© 2020, Walumbe Wapukha Denis**

## **DEDICATION**

This thesis is dedicated to my family. My parents have been encouragement and source of support in my journey. They taught me the value of faith and trusting in God. Above all, I cannot fully express my gratitude for priceless love and encouragement that my wife Bilha, Jason Carlos and Princess brought in my life.

## **ACKNOWLEDGEMENT**

The thesis could not have been possible without help and support of many people. I would like to express my sincere gratitude to my supervisors, Dr. Jotham Wasike, and Dr. James Ogalo for guidance and encouragement throughout the process. They provided excellent professional support and valuable comments on my research. I appreciate the University of Eldoret and Kibabii University for allowing me to carry out research data collection. Above all to God Almighty be the Glory and Honor.

## Table of Contents

DECLARATION OF PLAGIARISM.....	iii
COPYRIGHT .....	iv
DEDICATION .....	v
ACKNOWLEDGEMENT .....	vi
LIST OF TABLES .....	x
LIST OF FIGURES.....	xi
LIST OF ABBREVIATIONS AND ACRONYMS.....	xii
ABSTRACT .....	xiii
<b>CHAPTER ONE</b> .....	<b>1</b>
INTRODUCTION.....	1
1.0 Background to the Study .....	1
1.2 Problem Statement .....	3
1.2 Purpose of the Study .....	4
1.3 Research Objectives .....	4
1.4 Research Questions .....	5
1.5 Assumption of the Study.....	5
1.6 Significant of the Study.....	5
1.7 Scope of the Study.....	6
1.8 Limitation of the Study .....	6
1.10 Conceptual Framework .....	7
<b>CHAPTER TWO</b> .....	<b>10</b>
LITERATURE REVIEW.....	10
2.0 Introduction .....	10
2.1 Information Security .....	10
2.3 Insider Threat .....	11
2.4 Concept of Insider Security Threats.....	12
2.5 Motivations for Insider Threats.....	15
2.6 Impact of Insider Threats .....	18
2.7 Security Mechanism in Place in public universities .....	20
2.7.1 Classification of Security Mechanisms in Place.....	20
2.8 Models for Insider Threat.....	23
2.8.1 Domain Oriented Approach.....	23
2.8.2 Prediction Model .....	24
2.8.3 Intent-Driven Insider Threat Detection .....	26
2.8.4 The Nurse Prediction Model.....	28
2.8.5 Honeypot .....	37

2.9 Literature Gap .....	38
<b>CHAPTER THREE</b>	<b>40</b>
RESEARCH METHODOLOGY .....	40
3.0 Study Area.....	40
3.2 Research Design.....	40
3.2.1 Study Units .....	41
3.3 Quantitative Approach .....	42
3.4 Research Strategy.....	42
3.5 Sample Selection.....	42
3.5.1 Study Population.....	42
3.5.2 Sampling Technique .....	44
3.5.3 Sample Size .....	45
3.6 Data Collection Instruments.....	46
3.6.1 Questionnaire .....	47
3.6.2 Data Collection Procedures .....	47
3.7 Quality Control.....	47
3.7.1 Validity.....	48
3.7.2 Reliability.....	48
3.7.3 Pilot Test .....	49
3.8 Data Analysis .....	49
3.9 Ethical Consideration .....	49
<b>CHAPTER FOUR</b>	<b>51</b>
DATA ANALYSIS AND INTERPRETATION .....	51
4.0 Introduction .....	51
4.1. Response Rate .....	51
4.2 Missing Value .....	52
4.3 Reliability and Validity Tests.....	52
4.3.1 Cronbach Alpha Coefficients.....	53
4.4 Tests for Assumptions of Normality .....	54
4.5 Security Threats in the Universities .....	55
4.5.1 Establish Insider Threats in Selected public universities in Kenya.....	55
4.5.2 How the Respondents Know the Insider Attacker Incidents .....	58
4.6 Mechanisms in Place in Universities Against Insiders .....	61
4.7 Motivators of Insider Security Threat .....	67
4.7.1 Insider Attackers are Motivated by Financial Gains .....	67
4.7.2 Insider Attackers are Motivated by Disgruntlement.....	68
4.7.3 Insider Attackers are Motivated by Revenge .....	69
4.7.4 Insider Attackers are Motivated by Getting Attention .....	70
4.7.5 Insider Attackers are Motivated by Not Rewarded .....	71



4.7.6 Insider Attackers are Motivated by Lack of Promotion .....	72
4.7.7. Insider Attackers are Motivated by Espionage.....	73
4.8 Summary .....	74
<b>CHAPTER FIVE</b> .....	<b>75</b>
DISCUSSION AND CONCLUSION.....	75
5.0 Introduction.....	75
5.1 Discussion .....	75
5.2 Conclusion.....	81
<b>CHAPTER SIX</b> .....	<b>82</b>
RECOMMENDATION .....	82
6.0 Introduction.....	82
6.1 Proposed Insider Detection Model.....	82
6.1.1 The Elements Recommended for Removal in Next Model .....	84
6.1.2 Recommended Model .....	85
6.1.3 The elements of the model .....	86
6.2 Validation of the Insider Detection Model.....	87
APPENDIX A .....	97
Questionnaires.....	97
a. Information Systems Experts.....	97
b. Employees/Information System Users .....	103
APPENDIX B .....	107
Statistical Table for Determining Sample Size .....	107
APPENDIX C .....	108
Letters of Authorization and Permit.....	108

## LIST OF TABLES

Table 3.1 Study Units .....	41
Table 3.2 Sample Size of Information System Experts and Users .....	45
Table 4.1 The Rate of Response for Sample Population .....	52
Table 4.2 Reliability Test.....	53
Table 4.3 Scale Mean if Item Deleted .....	53
Table 4.4 Tests of Normality .....	54
Table 4.5 How they Heard or Knew About Insider Incident.....	58
Table 4.6 Action Taken Against the Insider Attacker .....	59
Table 4.7 Activities Carried Out or Aim of the Attacker .....	60
Table 4.8 Damage Was Done/Effects of the Insider Activities .....	61
Table 4.9 KMO and Bartlett's Test .....	62
Table 4.10 Total Variance Explained .....	63
Table 4.11 Factor Loading for Mechanisms Against Insider Security .....	64
Table 4.12 Factor and Mechanism used in Public University .....	65
Table 4.13 Insider attackers are Motivated by Financial Gains.....	67
Table 4.14 Insider Attackers are Motivated by Disgruntlement.....	68
Table 4.15 Insider Attackers are Motivated by Revenge.....	69
Table 4.16 Insider Attackers are Motivated by Getting Attention.....	70
Table 4.17 Insider attackers are Motivated by not Rewarded .....	71
Table 4.18 Insider Attackers are Motivated by Lack of Promotion .....	72
Table 4.19 Insider Attackers are Motivated by Espionage.....	73

## LIST OF FIGURES

Figure 1.1 Conceptual Framework of the Insider Security Threat .....	8
Figure 2.1 Framework of Insider Threat Model .....	25
Figure 2.2 Example of Document graph.....	27
Figure 2.3 Catalysts; Understanding the motivation to attack .....	30
Figure 2.4 Behavioral Elements.....	32
Figure 2.5 Motivation to attack.....	34
Figure 2.6 Steps of Attack .....	35
Figure 2.7 Actor Element.....	36
Figure 2.8 Attack Element .....	37
Figure 4.1 Users Witnessed or Aware of Insider Attack Incident .....	56
Figure 4.2 Activities Carried Out.....	57
Figure 6.1 Insider Attack Prediction Model By Nurse and Others.....	84
Figure 6.2 A Model for Predicting Insider Attacks .....	85

## **LIST OF ABBREVIATIONS AND ACRONYMS**

ANOVA:	Analysis of Variance
CERT:	Computer Emergency Readiness Team
CUE :	Commission of University Education
CSEI:	Centre for Systems Engineering and Innovation
CSO:	Chief Security Officer
CSI:	Computer Security Institute
CWB:	Counterproductive Workplace Behaviour
FBI:	Federal Bureau of Investigation
HVAC:	Heating, ventilation, and air conditioning
IT:	Information Technology
ICT:	Information Communication and Technology
ISO:	International Organization for Standardization
IEC:	International Electrotechnical Commission
MIS:	Management Information System
NACOSTI:	National Council for Science and Technology
SPRINT	Southern Pacific Railroad Internal Networking Telephony
SPSS:	Statistical package for social science
UoE:	University of Eldoret
USSNTAC:	Secret Service National Threat Assessment Center
US:	United States

## ABSTRACT

Insiders are the people with legal access to the information and poses a challenge to the security of the information systems. The insiders may compromise the system security through misusing the resources they have been assigned to accomplish their roles in the university. The study objectives were to establish information systems security insider threats in selected public universities in Kenya; evaluate insider system security mechanism in place in selected public universities in Kenya and update an insider system security attack prediction model for insider security threats. Two public universities were selected for data collection where information system users and information systems experts were targeted in a quantitative research approach. Questionnaires were used as research instruments in data collection. The study established that there were insider security threats in selected public universities with 55% of the respondents stating they had been aware of such incidents in their working stations. There were several reasons that were pointed out as motivators for insiders to initiate attacks. Financial gain, disgruntlement, revenge, attention seeking, not rewarded, lack of promotion and espionage were found to be motivators of insider attackers. The leading causes of insider threats were also explored where weak policy, and lack of implementation of the policies being the key causes of insider security threats. The study recommends a predictive model for predicting the insider attacks was realized out of the need for a precise and better prediction model where different components of the insider threat issue could be easily understood and implemented. There were several elements that the model proposed. The elements represent four areas; *the motivator* henceforth referred to as *catalyst*, *actor characteristics* (those of the potential insider threat), attack characteristics and the institution characteristics.

# CHAPTER ONE

## INTRODUCTION

### **1.0 Background to the Study**

Universities have always put forward the top notch tools, procedures and policies in the process of protecting its information systems from attackers and infiltrations from outside. Despite the amount of investment channelled towards development of infrastructure and manpower in guarding against the external aggressors, the universities still experience significant attacks causing greater loses. The security threats have been discovered to be from the inside the organization, this results into a complex and bigger exercise to handle. It is worth pointing out that employees are the greatest and most valuable resource of any company. Despite the fact that there is technological revolution and the internet of things, company staff are still paramount to the general success of the company (Olsen and Zaman, 2013).

Information system administrators of the organization are the most trusted employees that have all access rights with the responsibility to check and decide on the restrictions and access of the system resources. The administrators are best people for the organization to offer protection and security but they can also be the worst foes in disrupting security advances (Sterman, 2006). The same is true with the top management of the organization who have access to almost complete access to the entire resources of the organization. After this group, there are the middle-level and low-level employees that access company system resources based on their needs. There are different security mechanisms in place that security experts use in managing access to the system. The mechanisms include; technical, physical, and logical controls. Technological controls are the techniques that

include the use of firewalls, prevention systems, anti-virus and intrusion detection approaches. The logical controls include the access to the control policies like how users are authenticated and allowed to access specific resources and the access control policies and network management procedures among others. The physical control are about the policies and methods of only having authorized people to access the resources of the organization. They include the door scanners, employee entry-pass tags and entry guarding personnel.

Though there are technical and physical controls deployed by institutions to manage access to certain restricted resources, these measures are reactionary, only taking effect when insurmountable damage has already been done. Thus, it can be argued that they come second after the human element. A network access security policy can only be followed by an employee who follows rules (Dark, 2012). This is true for other technical controls such as log monitoring, firewalls, and honeypots among others. A dissident employee will find a way to circumnavigate the security policy no matter how strict it might be. When dissidence occurs with respect to laid down rules and policies, the psychological settings of employee changes, subsequently jeopardizing productivity. According to Perlow, (2003), employee resentment leads to decreased productivity and creativity which ultimately leads to loss of money, time and resources. Many organizations relay the information that dissent is discouraged whether verbally or non-verbally. However, a number of studies have corroborated Perlow and noted that receptiveness to dissent facilitates design of corrective measures to monitor unethical employee behaviours, impractical and inefficient organizational policies and poor and unfavourable decision making processes. Leading among all is the chance dissent accords

organizations to respond to insensitiveness to employees' occupational needs and requirements. Eilerman in Perlow, (2003) argues that the hidden overheads of silencing dissent include decreased job satisfaction and motivation reduced decision quality and lost time (Claycomb *et al.*, 2014).

This pinpoints the importance of human factor especially human resource and general management in devising and implementing workable security policies. With a pool of knowledge on human resource management, an organization can be better equipped to implement internal controls that monitor, detect and mitigate unauthorized access to restricted information.

This is a common problem overlooked by system administrators and only realized years after employee termination or when an attack has occurred. Before the digital revolution, security experts were kept awake at night worrying about the danger posed by untrustworthy members of their companies who had privileges to classified information and could easily usurp this opportunity to remove paper records from storage facilities and transfer them elsewhere.

## **1.2 Problem Statement**

Universities just like many other institutions have shifted to information system based processes and procedures in its operations. Critical operations like examination and finance, information about its clients and other stakeholders is stored on these information systems. There are universities that have shifted to online platforms and networked systems within the organization. The purpose of information systems such as enterprise resource planning system is to improve services. It is expected that employees and stakeholders would use the information systems in providing services as per the



strategic plans and objectives of the universities. They have been facilitated with the information system resources and authorization to access the resources. Legal and proper use of the resources is the aim of the of ICT integration to universities. However, there has been an increased trend where security threats and breach of the information systems coming from the trusted employees. They are people with valid authorization but have misused the privileges given to them. In most cases the systems security administrators discover the insider threats when the incidences have already occurred. The insider threats have put the examination integrity, university certificates, financial accountability and ICT resources into question. The impact of insider security threat largely affects the university on academic integrity, financial loss and general reputation of the institution. This study sought to present with a detection model that enables the Kenyan universities to overcome the challenges posed by insider security threats. By having a security model, universities should be able to detect security breaches before they occur. Currently, there are no models proposed or implemented at the university level.

### **1.2 Purpose of the Study**

The purpose of the study was to investigate the insider security threats detection mechanisms and develop a model for detection of insider security system threats in selected public universities in Kenya.

### **1.3 Research Objectives**

The following objectives guided the study:

- (i) Establish information systems security insider threats in selected public universities in Kenya

(ii) Evaluate insider system security model in place in selected public universities in Kenya

(iii) Update an insider system security attack prediction model for insider security threats

#### **1.4 Research Questions**

(i) What are the insider security threats in selected public universities in Kenya?

(ii) What are the security mechanisms in put in place against insider information systems security threat in selected public universities in Kenya?

(iii) Can prediction model for insider security threats be updated to suit selected public universities in Kenya?

#### **1.5 Assumption of the Study**

The study was carried out under the following assumptions:

(i) The ICT directorate of the universities have proper records for the insider security threats. This is important so that even if the employee that handled the incidents are no longer with the university, it is possible to get the file records.

(ii) The users are aware of the security policy and insider threats they pose to the universities

#### **1.6 Significant of the Study**

The study contributes to the current literature of insider security threats and mechanisms of detection. The security detection model that was modified is a significant contribution to the current models. The model that was modified be for learning institution since the current models are only for corporate custom sectors.

The study benefits universities and other institutions that are struggling with the insider security threats. The study is going to significant at this point where the

quality of university academic standards is being evaluated with the introduction on information systems. The quality of examinations administered to students and all the administration operations using information systems need to be beyond reproach. This study has developed a model that can be used to restore confidence of the stakeholders about university quality standards.

The universities are likely to save funds that are lost annually from the loopholes in the current mechanisms. If they use the model to predict the behaviour of potential insider threats. The model can be used not only in universities but also in other public and private organization in detection of the insider threats. The model is applicable in other sectors. The study is also essential for current literature on insider security threats; it contributes knowledge to the area of study for insider security mechanisms and detection models.

### **1.7 Scope of the Study**

The study focused on modified security threats model within two universities; Kibabii University and University of Eldoret the scope content was information security threats from the insiders. The context of the study was higher learning institutions that are selected public universities. The universities are located in Bungoma county and Uasin Gishu county and only the main campuses were used for study. The study did not include other satellite campuses that are within the same geographical location or in other counties. The study was undertaken within one academic year as it was time fixed for the researcher study.

### **1.8 Limitation of the Study**

The following was the limitation that the study faced or encountered.

- (i) The study depended on self-reported data. There was no independent verification of what an individual offers during data collection. It means that issues like selective memory where respondents remember given events were likely to occur. The respondents may not have shared information that implicates them or they were part of the issue. The respondents may choose to skip events that they are likely to be implicated or modify the events to suit themselves.

### **1.9 Delimitation**

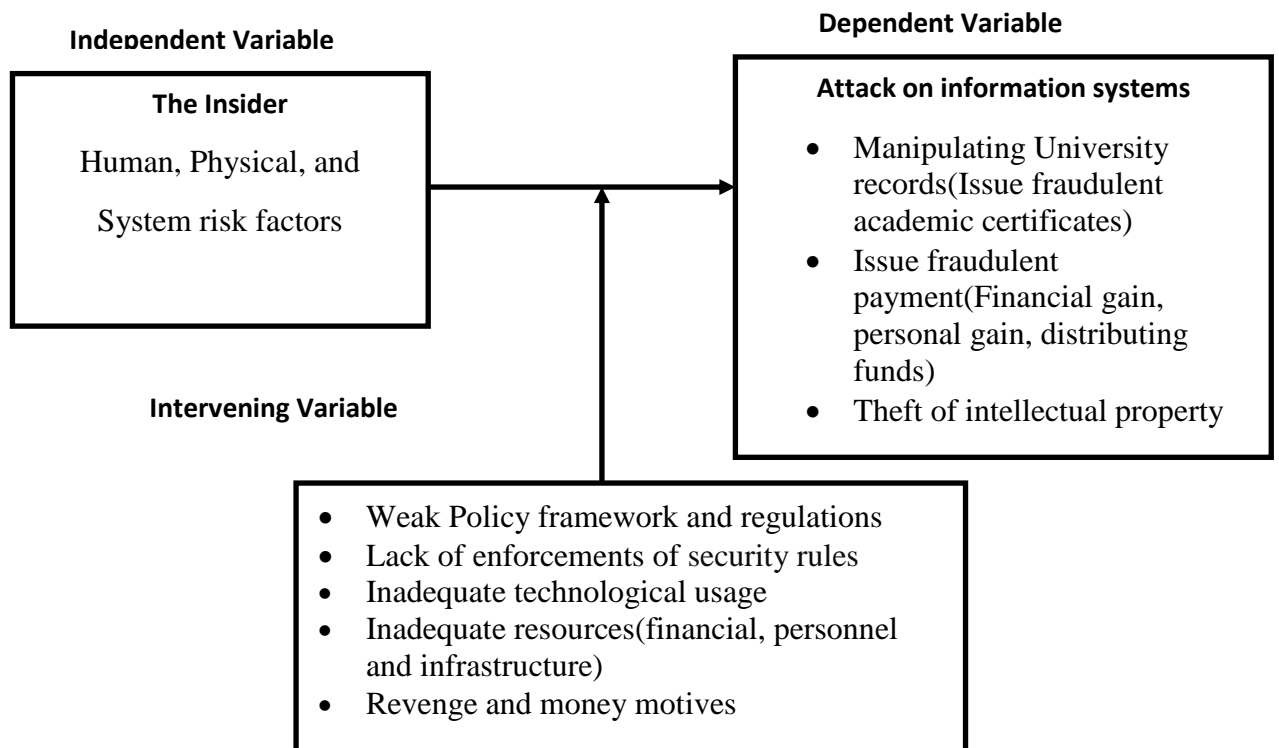
The researcher assured the respondents about the purpose of the research purpose as being for purely academic purposes. This was to ensure that they do not withhold information even if it implicates them directly. They were further assured that no personal details were need that was to be used to link directly to them. The information was not to be shared by the institution authorities hence they were not going to be victimized for sharing information. This assurance gave them confidence to respondent without being afraid of the consequence.

### **1.10 Conceptual Framework**

The conceptual framework for the insider security threat is derived from the variables of the research topic. The conceptual perspectives were mainly about the insider characteristics and motivations, the insider threats and the possible impact of the insider attack. The intervening variables are the policy weakness and failure to effectively implement the policy. The practical perspectives are about the best practices for information systems security evaluation as presented by ISO/IEC 15408. The insiders resulted into threats which took advantage of the weakness of security measures in place. The figure below combines both the theoretical and practical perspectives to a conceptual model which is a representation of the insider security threat. It includes aspects that have

been explored in literature review. The model provided by Nurse et al. (2014) was used in modified the current conceptual framework as it was the model that the study modified as recommended solution for the study.

The study conceptual framework



**Figure 2.1 Conceptual Framework of the Insider Security Threat**

Source (Researcher, 2016)

The insider in the model is the agents and factors that lead to insider treats being present. It is the humans working within the organization that are insiders while physical systems presents the actual factors to the risks. The listed intervening variables such as weak

policy, inability to enforce the security policies, lack of resources towards security and motives to the insider actions are the intervening variables. The combination of the independent and intervening variables gives the results of the information systems in case they are present for the organization. The dependent variable only occur based on independent variables and intervening variables. The organization is likely to security breach that results to manipulating university records where insider can issue fraudulent academic certificates or modify exam results. Issuing of fraudulent bank cheque results to financial loss.

## CHAPTER TWO

### LITERATURE REVIEW

#### 2.0 Introduction

This chapter covers the previous studies on insider security threats. The insider threat literature review looks at the definition of the insiders in the context of information security systems threats. Contrasting, similar and parallel studies on the factors and motives for insiders to attack the information systems or circumnavigating policy systems, the insider detection models and were reviewed from the previous studies.

#### 2.1 Information Security

Currently, institutions are using information systems to store, manipulate and disseminate valuable information asses. Draft (2000) defines information as data that has been processed into meaningful and useful context for the users. What is considered valuable information depends on the organization, but it includes strategic information and intellectual property for an institution like universities used to gain competitive advantage over the competitors. According to Ezingear *et al.* (2005), confidentiality is about accessibility on the need to know basis and the authorization access to the information.

Hunker & Probst (2011) states that an insider is considered based on the organization. Organizational policies and values together with the system specific characters are used in defining the insider. The table below shows the definition of an insider from the peer review articles of insider threat.

There are several definitions of the term insider for security threat. As per Carroll, Greitzer & Roberts (2014). “[...] what is meant is any and all persons that have access to an organizations information including people such as contractors, temporary employees and the like.” While Bishop, et al., (2014), adds that an insider is “Anyone with access, privilege, or knowledge of information systems and services.” He adds “[...] anyone operating inside the security perimeter.” Closely linked study by Schultz (2002) brings out another aspect of insider as “[...] insider: would usually be employees, contractors and consultants, temporary helpers, and even personnel from third-party business partners and their contractors, consultants, and so forth.” On the other hand Hunker & Probst (2011), expands the list of insiders “Insider: someone with legitimate access to an organization’s computers and networks. For instance, an insider might be a contractor, auditor, ex-employee, temporary business partner, or more. ” Mills, et al., (2011) sum up the definition of the term insider as “[...] an insider is any individual who has been granted any level of trust in an information system.”

### **2.3 Insider Threat**

The threats to vital information emanate from the external and internal threat agents. Baker *et al.*, (2008) states that although there has been a lot of publication on external threats such as hacking and viruses, insider threats have gained grounds and are at higher level of risk.

The following are existing literature on the definitions and description of the terms insider threat or insider attack.



Bishop, et al. (2014) Insider attack “malevolent actions by an already trusted person with access to sensitive information and information systems.” Additionally Carroll, Greitzer & Roberts (2014) adds that the “Insider threats can be either intentional or unintentional.” Schultz (2002), presented a longer version on understanding insider attack as “An insider attack is considered to be deliberate misuse by those who are authorized to use computers and networks.” “[...] insider attackers are those who are able to use a given computer system with a level of authority granted to them and who in so doing violate their organization’s security”. The insider attack is about the misuse of the resources which is carried out by the insider which can be successful or not. The attack is about several events or actions that result into use of information in a manner that contradicts the security policy of the institution (Bishop *et al.*, 2014). The insider threat is that possibility of the insider to carry out the attack. The insider can either exploit the security system intentionally or unintentionally (Nostro, 2014; Schultz, 2002).

#### **2.4 Concept of Insider Security Threats**

This section explores the concept of insider security threats as presented in different literature. With the main focus on the classes of insider threats, motivation and what impact they may cause for the organization. According to Baracaldo & Joshi (2012), an insider threat is an associate of a company in form of employee, contractor, business partner or sponsor who is authorized to access an organization’s network, system, physical location or data and intentionally misuses those privileges to alter confidentiality, integrity and availability of organizations information for their own benefit (Claycomb *et al.*, 2012). Insider threats involve such activities as espionage,

fraud, theft and sabotage conducted via varied mechanisms such as access privileges abuse, theft of organizational resources and mishandling of physical materials (Baracaldo & Joshi, 2012). Insider threats can be malicious or unintentional meaning that actors do not recognize that they are aiding a threat. Insider attacks have been blamed for numerous losses in public and private organizations amounting to billions of dollars of revenue (PricewaterhouseCoopers, 2012). Apart from financial aspects, there are trust issues associated with business partners, contractors and customers (Claycomb *et al.*, 2012). As a result, it is a vice that eats the company from within impeding growth and establishment of a fair competitive arena. It is paramount that organizations recognize normal employee action baselines and advance such knowledge to employees so that they can understand when they are used by others as conduits to obtain information (Baracaldo & Joshi, 2012). Practically, there are near-infinite employee types in an organization. However, most employees fall within one of the four primary classes. This classification of employees is based on behaviours as it presents a powerful tool to dealing with security challenges (Crawford & Peterson, 2013). Generally, employee classification has resulted to the following: citizens; these are employees who follow regulations set aside by the company in accessing resources. They seldom use technological resources for their personal use other than assigned tasks (Boender *et al.*, 2014). This group of employees are proactive in security management and do not get involved in insider attacks. Delinquents and Renegades; Delinquents are aware of acceptable use policy as well as other regulations governing resource use in the organization. However, they deviate to take small liberties such as checking their personal mail, shopping online and playing computer games. They can also install some software to assist them in checking their

performance of legitimate activities (Boender *et al.*, 2014). This group of users are technology-savvy and may extend their authority to assisting others in their execution of technical aspects, hence unintentionally gaining access to resources not meant for them (Boender *et al.*, 2014). They are generally accorded respect by co-workers because of their advanced computer skills and sometimes, may overstep their authority by acting recklessly or negligently.

This groups of employees spent a considerable amount of time doing this that they are not required of them. Hence, they tend to abuse Internet privileges, undertake personal projects among others. They are careless with company data and are more likely to exploit loopholes in policies and procedures for their own sake (Boender *et al.*, 2014). Though they might not directly attack the company, their priorities is not in line with that of the employer and consequently endanger company assets and information. Rogues and Multi-class employees; these are employees who continuously endanger company's confidential information for financial prospects. They differ from all the groups discussed above because their prime motive is benefiting from the insecurities of the organizations (Claycomb *et al.*, 2012). It is notable that most of the damaging insider attacks were likely perpetrated by rogue employees

While it is common for employees to behave true to their nature and class, some changes class depending on the impending conditions (Boender *et al.*, 2014). A renegade who was subjected to disciplinary action may choose to be a citizen while a citizen who has been subjected to negative restructuring events may turn rogue.

## **2.5 Motivations for Insider Threats**

Over the years, extensive knowledge has been explored on ways of countering the insider. Centuries of studies indicate that insiders are motivated by financial prospects, ego, coercion, and ideology (Magklaras & Furnell, 2001).

The motivations for insider attacks are event-specific. Generally, these motivations have been classified as follows: financial gains; financial gain is considered one of the prominent motives for insider activities. Theft and sale of employer's confidential information to competitors, stealing co-workers financial data for personal use and manipulating company's financial information in exchange for monetary gains is found common in people in financial, banking and insurance companies (Boender *et al.*, 2014). According to studies conducted by USSNTAC and CSEI, 81% of the insider threats were motivated by financial gains other than the motive to harm information systems of the company. Of the insiders studied, 27% of them were experiencing financial constraints and decided to sell company information to get more finances (Boender *et al.*, 2014). In one scenario, a currency trader modified software with capability to record, manage and audit trades. The software was made to be highly secretive such that auditors find it impossible to detect it.

Disgruntlement; the causes of disgruntlement in an organization are attributed to many factors including aggressiveness towards co-workers, subordinates and supervisors. Usually, management, organizational culture and hanging company policies make it hard for employees to adapt to new environments and hence the frustration and thought of harming the company (Magklaras & Furnell, 2001).

A case demonstrating this is an employee who was asked by the company to develop an internet website because of his graphical programming skills. After few months, the employee was reprimanded for absenteeism and the company executive issued a directive for the employee to be suspended (Boender *et al.*, 2014). Later in the day, the employee accessed the company's server deleted all information and added different texts and graphics to the website. Upon investigation and prosecution, the employee admitted to have committed the offense out of fury for being suspended. Statistics conducted by USSNTAC and CSEI in 2005 revealed that 85% of insiders have unresolved issues prior to committing the offense (Claycomb *et al.*, 2012). 92% of the grievances involved employees, supervisors and co-workers and the more a company is adamant to resolve it, the more the grievances the higher the risk of insider activities.

Espionage; it is another motive for insider activities. Espionage is committed by a spy or a mole that is influenced by targeting the company. The spy conducts surveillance activities by installing software, cameras and microphones at distinct locations which they use to monitor the actions of other employees and consequently steal confidential information, company records, and employee personal information (Boender *et al.*, 2014). The insider has access to information about its company such as security and surveillance systems. The insider is used by the attackers outside the organization as leverage to facilitate theft of information (Claycomb *et al.*, 2012). In most cases, criminals entice employees into perpetrating attacks without even the employees knowing. Competing companies consider espionage as a safe method of spying on their competitors rather than attacking since their reputation is not affected in the long run.

Revenge; second to financial gains is revenge. An insider with negative feelings about the company and other employees will seek revenge by attacking the company and its resources. Executing revenge require proper planning and patience for the right time (Boender *et al.*, 2014). It requires gathering sufficient information about the targets and waiting for an appropriate moment, thus, avenging employees would execute their activities after exiting the company.

Curiosity; certain employees in the company are curious of their surroundings and would like to expose it to the world whereas other considers it as a challenge to prove a point to themselves and others (Boender *et al.*, 2014). Consequently, in their course of activities, they disregard company security policy and play around with the resources, bypassing security protocols and accessing unauthorized resources. This crop of employees are especially young and out of college, keen on experimenting and learning a few concepts and technologies (Claycomb *et al.*, 2012). In a bid to prove themselves better than co-workers, they launch attacks, modifying company resources or stealing information.

Emotional Distress; According to Boender *et al.* (2014), people who have done through rough phases in their lives develop frustrations towards the society. Emotional distress is as a result of a number of factors including work pressure, family issues and lack of social skills (Boender *et al.*, 2014). Emotionally distressed employees are isolated, withdrawn and portray negative attitudes towards life. Thus, they are more likely to strike at the system to justify a purpose.

Desire for Respect; every employee in an organization has particular skills with which it is respected accordingly by co-workers. However, some employees possess advanced skills while others have less skills but the whole set is considered part of the core

company. Boender *et al.*, (2014) affirms that in times of adversity for example during layoffs, less skilled employees are the once to go first or during deliberations, their opinion is given least consideration. As a result, these employees would want to prove a point to co-workers to demand respect and consideration (Magklaras & Furnell, 2001). While some employees work hard to advance their skills, others work hard to commit malicious activities to justify a cause. (Claycomb *et al.*, (2012), states that other motivations for insider attack in an organization include decision failures and mental problems.

Hong (2010) asserts in the custom, information security aspects in private and public organizations have been geared towards external threats, whilst significantly ignoring internal threats originating from within. The common assumption was that the risk and likelihood of internal threats was minimal in comparison to external threats. However, history has proved that internal threats are detrimental and costly to the organization (Hong, 2010).

## **2.6 Impact of Insider Threats**

According to the agency, insider threats involve among others, fraud, theft of intellectual property, IT sabotage and espionage. To illustrate how each of these examples can lead to denial, degradation, disruption, destruction, deception and corruption of company information, a case is presented.

A software developer at a credit card company devised a fraudulent mechanism of awarding himself reward points by linking his personal accounts with corporate business credit card accounts of external companies. He cashed in the accumulated points for gift vouchers and subsequently sold them in online auctions sites for cash (Claycomb *et al.*,

2012). Before being caught, he had accumulated a total of 40 million reward points which translated to \$250,000. His fraudulent actions were unearthed by internal fraud detectors (Baracaldo & Joshi, 2012).

A US company developing pigments used in paints, plastics and paper had its intellectual property stolen by a Chinese company. Chinese state-owned Pangang conspired with the US original company's employee to steal intellectual information used to build a 100,000 annual-metric-ton pigment production plant (Crawford & Peterson, 2013). The US naturalized employee had spent 35 years with the company and had extensive knowledge of manufacturing and trade secrets which he released to Pangang. This led to subsequent losses on the part of the original company amounting to billions of dollars and unemployment.

A health facility employed a security contractor to take care of security matters during the night. The security contractor happened to have been extensively involved in cyber malpractices and hacking albeit secretly. He utilized his security credentials to gain access of the physical computers that controlled HVAC systems in the facility (Crawford & Peterson, 2013). Using a number of techniques including password-cracking utilities, botnet and others, he rendered the HVAC system unstable resultantly leading to an outage for several hours (Claycomb *et al.*, 2012). The insider and his team were planning a distributed denial of service attack against an unknown party. Fortunately, a security researcher exposed their online advances and alerted the facility which led to arrests and legal actions.

A former Air Force intelligence specialist was detained as he was boarding a flight destined for Switzerland with information on missile information sites in Iraq. After a



search on his home computers, letters offering to sell secrets to Libya, China and Iraq was revealed. In respect to Iraq, the perpetrator had asked Saddam Hussein regime for \$13 million (Magklaras & Furnell, 2001). Investigation revealed that the specialist not only he been motivated by monetary gains, but also a sense of disgruntlement as he constantly complained to his co-workers and neighbours about his job and station. Information extracted after conviction lead investigators to 19 locations in rural Virginia and Maryland which had thousands of pages of classified information, videotapes and CDs presumably stockpiled for future sales.

## **2.7 Security Mechanism in Place in public universities**

These section presents how the measures are classified and how they have been used in different environments based on the specific insider threat presented to the organization

### **2.7.1 Classification of Security Mechanisms in Place**

The insiders who take advantage of the information system weakness on the security policy or measures are the insider threats. Security policy on the other hand is aimed at reducing the weaknesses that results into the system risk of information misuse. In the end the security policy may present weaknesses that lead to other risks (ISO/IEC 15408, 1999).

The current literatures have put more weight on the concept that information security is not an issue of technical measures (Carroll, Greitzer & Roberts, 2014). Information security is about the people, organizational factor, technology and the working environment. There are three types of security controls that have been proposed to deal with all aspects of information security:

*Formal control* this is about the organizational structure and an operation which ensures that there is proper conduct of business and minimizes the chances of an incident or an attack or at least reduces the impact. The control measures may include putting different departments for security and IT with clear roles of the departments to ensure proper control of the systems (Carroll, Greitzer & Roberts, 2014).

*Informal controls* are just the organizational culture, value and belief systems on the institution. It is where an organization through the management has shared vision and contribution towards achieving the vision is done by all the members. The organizational members are committed to seeing the vision accomplished. Increased trust and awareness of security issues for information system are some of the approaches that can be used in creating informal controls (Carroll, Greitzer & Roberts, 2014).

*Technical control* it is the mechanism that gives protection to the information systems from any kind of attack or incidents. The organization can use recovery and analysis applications, access control mechanisms, use of antivirus software among other mechanisms (Melara *et al.*, 2003).

Although each of the above control is important, they must complement each other (Carroll, Greitzer & Roberts, 2014). The search study by Martinez-Moyano *et al.*, (2008), confirms that successful defense against the insider threats demands that technical and behavioral solutions be implemented.

There are other ways in which controls or measures are classified apart from formal, informal and technical controls (Schultz, 2002, Carroll, Greitzer & Roberts, 2014).

*Prevention*, it is a measure aimed at removing any chances of occurrences of an insider threat. It includes measures which can be able to predict the insider attacks by looking at the potential indicators. As per Carroll, Greitzer & Roberts (2014) government agency regulatory forces the organizations to come up with such risk management methods. The internal security policy that for regulatory compliance and insider prevention, the internal policy behaviour and actions those employees in the organization should adhere to. But if the policy itself has limitations where it is not enforced with strong consequences then it is not useful. The consequences are important in keeping away insider threat (Carroll, Greitzer & Roberts, 2014).

*Detection* it is a measure that offers means of knowing that there is an insider threat when it has already happened. There are several tool and methods for outsider attacks detector where insider attack occurrence is not easy to detect (Carroll, Greitzer & Roberts, 2014). The insider can delete the actions to cover up the illegal actions carried out which makes it difficult to detect (Carroll, Greitzer & Roberts, 2014). Tools such as logging, honey pots, monitoring and whistle blowers are being implemented.

*Response* is another measure that is expected to detail how to respond after the insider attack has actually happened. The institutions are expected to take responsive actions against the insiders. It may be a simple solution of lawsuit for the company. In reality, it is not simple to respond to insider threats with lawsuits. The need for organizations to keep such events from public eye or bad press is what results dealing with the issues internally (Carroll, Greitzer & Roberts, 2014). There are many lawsuits where the organization is not likely to recover the damages but only punish the insiders. Although such actions may seem good in the public eye, recovering of lost assets, bad press and

effects on stock market for publicly listed company is not possible (Carroll, Greitzer & Roberts, 2014).

Although detection of insider threats just like the external threats is more preferred, in nature it is a post hoc approach (Schultz, 2002). According to Schultz, the most pressing need is developing a framework for predicting insider attacks. This is the aspect that the research seeks to address the urgent need of developing a model. There are several indicators discussed which can be modelled into a framework that can be used to predict insider attack.

## **2.8 Models for Insider Threat**

This section presents the existing research study insider security models that are being used for prediction and prevention of occurrence of insider threats. The previous studies have developed several models of insider security systems.

### **2.8.1 Domain Oriented Approach**

Qutaibah and Panda (2008) presented a domain oriented approach in predicting and mitigating an insider threat (Qutaibah and Panda, 2008). The approach presented states that the internal resources that an insider can access is denoted by  $s$ , where the insider can take more organization information. Access to company information gives the insider a chance to access confidential information, if the insider has malicious intent. The authors states that the knowledge that the insider has on how to access confidential information need to be controlled.

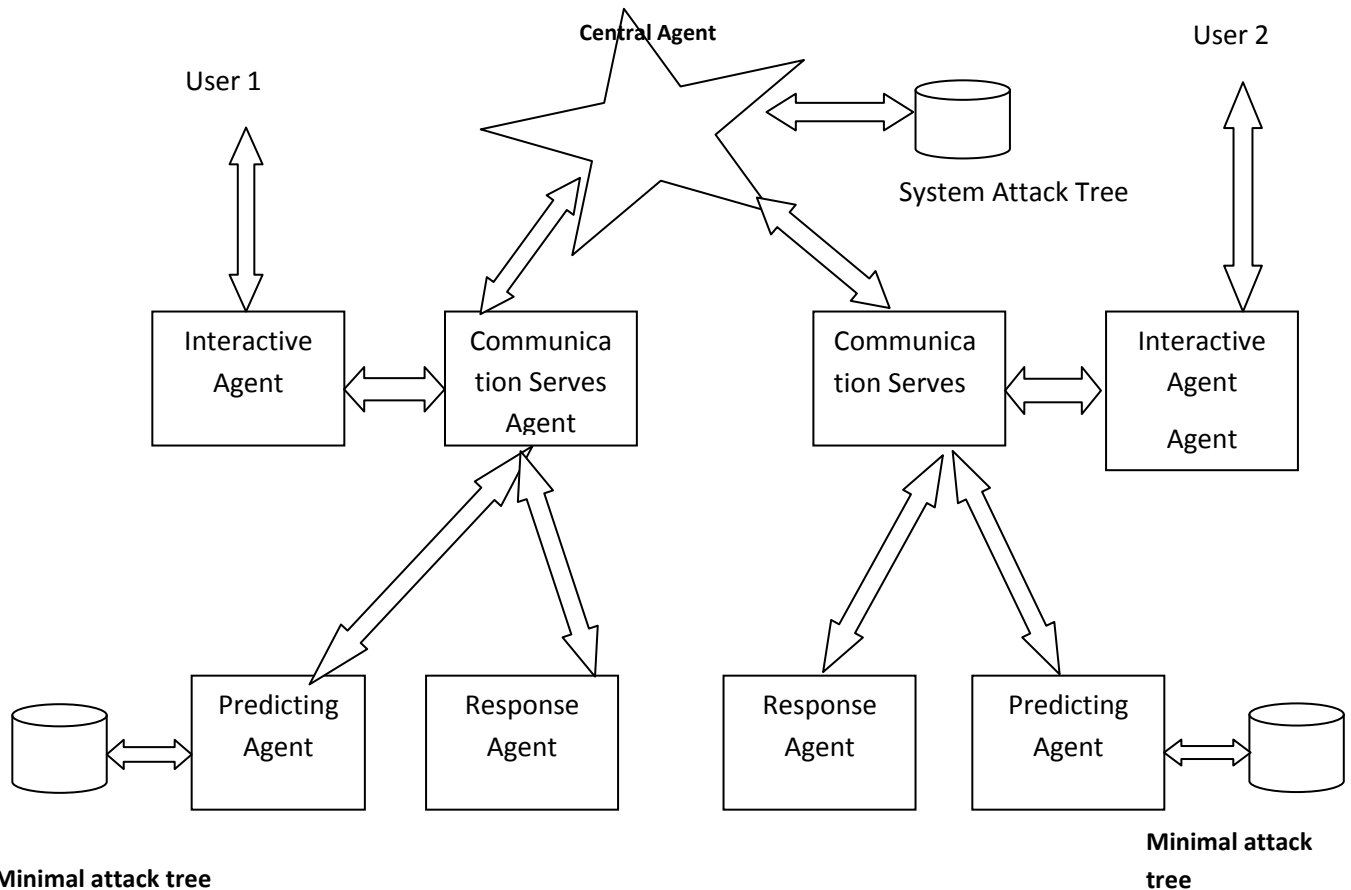
The weakness of the model is that it depends on the knowledge level as a means granting access to users. It means it does not detect even those with required knowledge and

would like to access information resources for personal gain. However, the model is credited for its simplicity in implementation.

### **2.8.2 Prediction Model**

Wang, Liu and Zhang (2006) proposed a model for prediction of the insider threat using a tree structure (2006). The authors used in their paper the attack tree that was introduced by Bruce Schneier (1999) in defining their model. The attack tree can be used for both internal and external attacks. The scholars came up with the Systems Attack Tree configurations after analysis of all the attack paths in the system in order to detect the insider threat.

The scholars state that if we are able to understand the intents of the insider access to the internal resources, then it is possible to intercept and detect insider threat. The insider offers reasons for access to the system before being allowed to access the system. The table known as the Signature Powered Revised Instruction Table (SPRINT), is set and the system makes Agent Observes (Aos), that is the operations the insider would like to perform in the system based on the SPRINT plan. The Minimal Attack Tree generated by Aos is used to make security systems detection of the malicious intent. The figure below shows the setup for insider detection.



**Figure 3.1 Framework of Insider Threat Model**

**Source: (Wang, Liu and Zhang, 2011)**

From the Figure 3.1 Framework of Insider Threat Model above, at the time of connection to the system by the insider, there are interactive agent requests for information on why the user has to access the resources and the n users have to wait for some time. The systems gives information to the user after configuration the Central Agent generates the Minimal Attack Tree after making a comparison with the System Attack Tree. The

Prediction Agent Observes the behaviour of the user by the Minimal Attack Tree to analyse the chance of attack. The user behaviours are stopped if the system detects any malicious intent.

The model presents several strengths such that there are observers monitoring the use of resources. However, it affects the concept of availability since the agents must be online to enable the access to the resources. Additionally, there is always change in behaviour of the information systems users when they are being monitored. Such is likely to affect creativity and room for mistakes on the system.

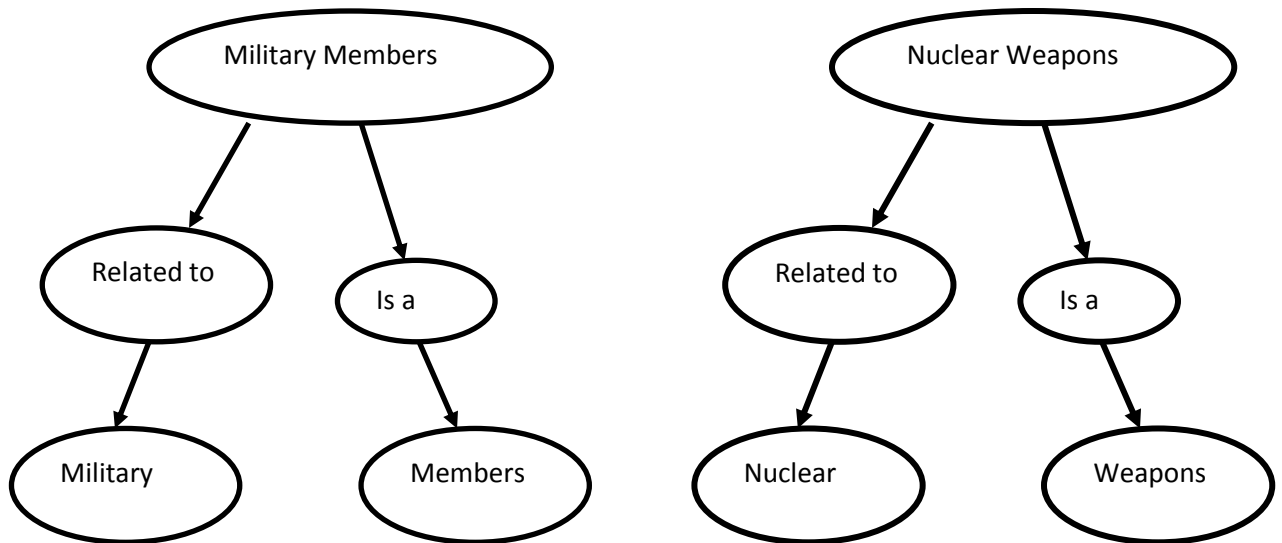
### **2.8.3 Intent-Driven Insider Threat Detection**

Santos *et al.*, (2008) presented an intent-driven framework that has s users of the model and insider detection metrics. The model automatically detects the insider threat (Santos *et al.*, 2008). Although the traditional studies on insider threats have put more weight on social network, document based and action based, the researchers focused on understanding the intent of the user.

Users have intention whenever they access the internal resources be it malicious or not. For one with malicious intent, there are some features that the mode presents (Santos *et al.*, 2008) such as use of many queries that are not supported, use documents that are old when there are no supporting documents, fabrication of information; when making reports and overstating some of the record information. It is through experiments that the insider intent is understood and classified accordingly.

The authors used the IPC model 1 (Nguyen *et al.*, 2004b; Santos *et al.*, 2003a) in coming up with the framework that contains the list of interest, preference network and context

network. The context network is most critical one. The document graph (DG) is used to model the knowledge context of the user.



**Figure 3.2 Example of Document graph**

**Source: (Montes-y-Gómez, Gelbukh & López-López, 2000)**

From the figure 2.4 above DG example, there are nodes and relationship between the nodes. There are two types of relationships ‘Is a’ relation and ‘Related to’ relations. The similarity between the documents accessed and the context network is computed using the following equation (Montes-y-Gómez, Gelbukh & López-López, 2000):

$$similarity(DG1 + DG2) = 1 + \frac{n}{2N} + \frac{m}{2M}$$

Where

**n** is the number of concept nodes as shared by DDG1 and DDG2

**N** is the total number of concept nodes in DG1



**m** is the number of relation nodes as shared by DDG1 and DDG2

**M** is total number of relation node in DG1

The DG presents a good approach of having a quick look at the model and the intent of the users of the information systems. The weakness of the model is that it does not address the aspect of information system users that become insiders by accident. They did not intent to access the files or use them for what reason but when they opened the files they then developed the intent. The intent coming after right reason for file access is not well addressed in the model. Additionally, implementation of the model requires more resources by the organization where there is an emergency. There is need to approve the access to the resources at any point.

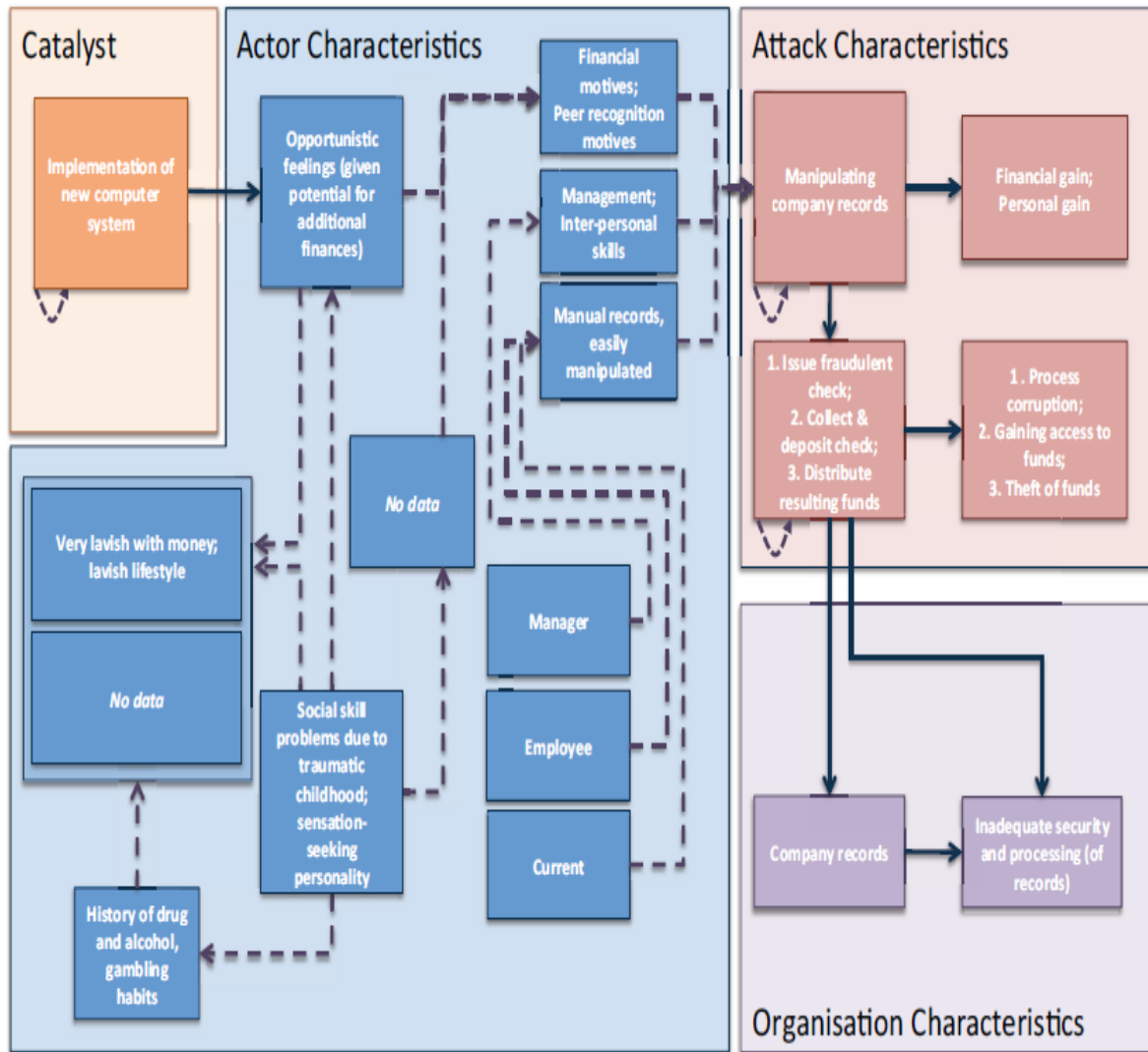
#### **2.8.4 The Nurse Prediction Model**

##### **The elements of the model**

The model presented in figure below is made of several components that will be referred to as *elements*. The elements represent four areas; *the motivator* henceforth will be referred to as *catalyst*, *actor [insider] characteristics* (those of the potential insider threat), *attack characteristics* and the *institution characteristics*. The insider as defined in the study will hence forth be referred to as actor. Specific elements are represented by the use of boxes while the solid arrows indicate the relation between elements with dashed lines indicating the potential associations. The study has further broken down the model into sections with the aim of simplifying the discussion and implementation of the model. The main sections of the models are; understanding the motivation to attack; observing the behavior of trusted personnel, the actor, dissecting the attack, the resources (information systems) under attack and their vulnerabilities.

### **i. Understanding the motivation to attack**

In order to explain the model elements, it is important to understand the behavioral and psychological aspects associated with the *actor/insider*; it is viewed as the password to knowing the motivation behind the imminent information systems attack. The behavioral and psychological aspects of the potential insider have been given attention by the researchers and practitioners hence the key findings of those studies was used (Micki Krause Nozaki, 2011). The catalysts in the study were cauterized as the leading causes, the individual characteristics; the psychological state and the motivation to attack were the aspects that are modeled in the study. The aspects are further discussed under each section and the relationship between them is considered.



**Figure 3.3 Catalysts; Understanding the motivation to attack**

Source: (Nurse et al., 2014)

**Precipitating event (Catalyst)**

They are the catalyst that has an influence on the insider which can tip them to become threats of the information system. As per the literature the participating events are referred to as ‘tipping point’ (Moore et al. 2008). A significant aspect that was evident from the study was that most of the attacks were based on perception or rumors of something bad that was about to happen as indicated established by (Wallnau, 2013).

### *Personality characteristics*

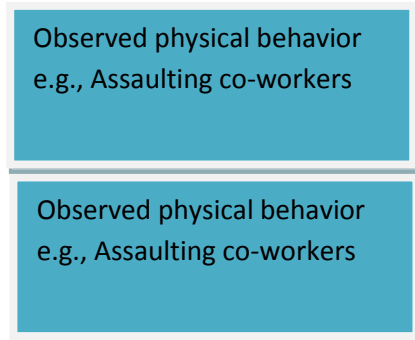
Personality characteristics, this is the psychological traits and dispositions that make the personality of the insider both as self and work experience. The self-aspects are static since they are innate while life experience is dynamic and more responsive. The personality traits include the openness. It was measured in the study by looking at the ability of the systems users to share password with others. There are other characteristics as per Qutaibah & Panda (2008), like social skill problems, superficiality, self-esteem, personal integrity, aggressiveness and maturity that can be used in understanding the personal characteristics.

Since it concerns the insider threat, personality characteristics are significant to how the humans think and act; hence they have a strong influence on the individual's involvement in malicious activities or behavior that exposes the system's vulnerability. The study emphasized more on personality traits by looking at the characteristics of the insiders before the incident happen. Personality characteristics in previous studies using many cases have been validated as having influence on insider attackers. Attention seeking or excitement seekers have been found to be high insider threats and antisocial behavior (Wood, 2000; Stavrou et al., 2014). There are information system users who are having the characteristics of agreeableness and openness that are likely to be scammed (Team, 2013).

### *Historical behavior*

The historical behavior was not subject of the study but the previous studies have extensively looked at the extensively. According to Qutaibah & Panda (2008), the type of activities that the insider has engaged in the past is likely to influence the personality

characteristics. According to Rauthmann et al., (2015), issues related to carelessness and absent-mindedness were discovered to be source of accidental, unintended insider threats.



**Figure 3.4 Behavioral Elements**

Source: (Nurse et al., 2014)

### ***Behavior elements***

There are many behaviors that are associated with personality characteristics. According to CMU-CERT in their case Caliendo, Fossen & Kritikos, (2014) they show the significance of this element where the systems administrator who had a history of electronic crimes employed similar techniques on the employer through blackmail and sabotage. Although it could be argued that background checks can be done on potential insiders before they are given access to resources in the institutions, the challenge is that universities may not have sufficient investigative capacity for a proper background check.

### ***Psychological state***

The insider psychological and emotional state such as stressed, depressed, happy, or anxious might be important factors influencing the insider attacker (Qutaibah & Panda 2008). Nozaki (2015) states that this element can be as a result of psychological make-up or environment related like stressful event, that explains the link with personality characteristics and catalyst event. Issue from workplace or outside the environment can

cause the state. As per the literature and the research results, disgruntled employee was found to be responsible for attacks. However, disgruntlement was only one of the states established as strong in the research to associate to insider attackers. The other factor from the study was lack of reward or appreciation that can influence the insider to be a potential insider attacker.

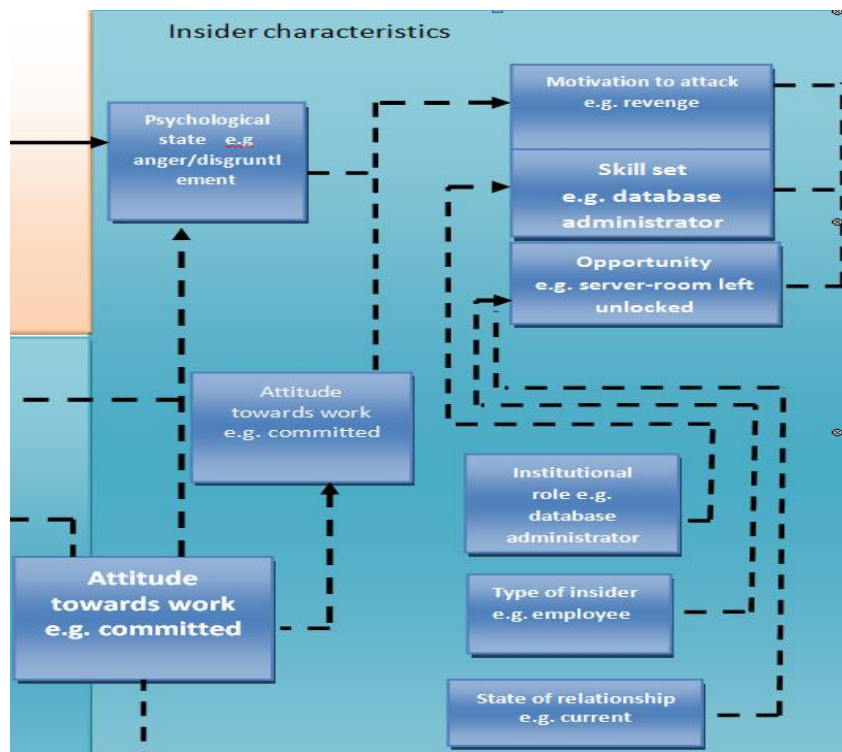
#### *Motivation to attack*

The motivation to attack was categorized as a section in order to explore the relationship with the precipitating events and the other elements of the model. The study came up with findings on the motivating factors that can also be found in previous studies (Santos et al., 2008, Spitzner, 2003, Wallnau, 2013) Motivation can be financial, political, revenge, curiosity or fun, competitive advantage, or peer recognition. Based on study findings financial gain, sabotage, revenge, and seeking attention were the main motivators of the insider attackers. As per the study, the psychological state has a significant influence on the motivation to attack.

Additionally, psychological state can work together with *Attitude Towards Work* in further influencing the insider. The study findings of (Bellovin, 2008; Bishop, 2013) further explains the link between attitude to motivation. Motivation in the study was classified as deliberate or accidental to ensure that the model is able to capture all types of insider threats.

The *skill-set* is also critical for the study since insider attackers without knowledge on how penetrate the system is not likely to initiate attacks where resources are protected. The attacker need to have the requisite skills to carry out an attack (Boende et al., 2014). A case from CMU-CERT shows that the software development background enabled the

insider to plant a logic code in the system software. The studies in the literature have also explored the concept of the chance to initiate an attack.



**Figure 3.5 Motivation to attack**

Source: (Nurse et al., 2014)

## ii. Observing behavior of trusted personnel [insiders]

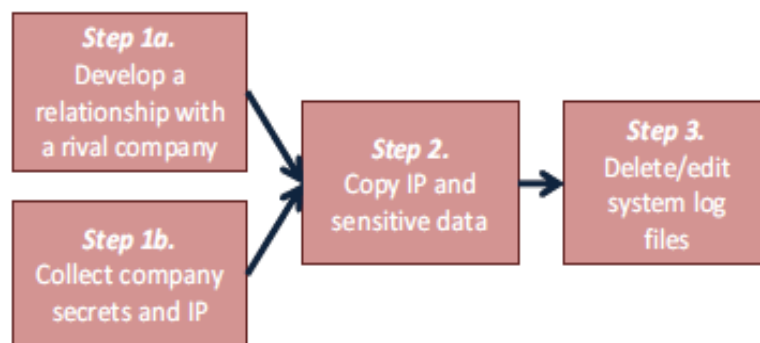
Observation in the model looks at monitoring the physical and cyber behavior of the insiders. *Observed physical behavior* might capture the physical behavior exhibited by the insiders such as accessing the building and other resources. *Observed Cyber Behavior* is about monitoring technology related behavior that an insider may show over the institution information infrastructure like the use of internet, email and workstations. The two observed behaviors are indicative of the potential attack either being done or about to happen.

## iii. The Insider

The term insider has been defined in literature citing from different scholars (Nostro et al., (2014); Gunasekhar, Rao & Basu, (2015); Schultz (2002); Carroll, Greitzer & Roberts (2014) and Bishop, et al. (2014). The insiders can be the employee, contractor, vendors, consultant, client and business partner. The external attackers should also be considered since they may recruit and work with trusted personnel to help in conducting an attack on the institution. The recruiter may be motivated by financial gain which has been established in the study and other studies as being a motivator for an attack

#### iv. Dissecting the attack

The attack is the activities that are done by the insider, either accidentally or deliberately that will negative affect the university. The attack outcome will be linked to the objective of the attacker. The external attacker should be considered in the model since they can recruit the insiders who are driven by the financial gain they may collaborate with the external attackers in exposing the system. The steps of attack are similar to those of the existing pre-defined notion of Attack Tree by Kammüller, Nurse & Probst, (2016) where there is a clear sequence of events before an attack. The Intrusion Kill Chains Hutchins et al. (2011), has relevance when looking at the Attack Steps.



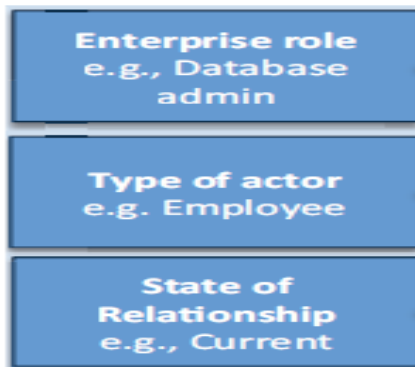
**Figure 3.6 Steps of Attack**

Source: (Nurse et al., 2014)



*v. Resources under attack*

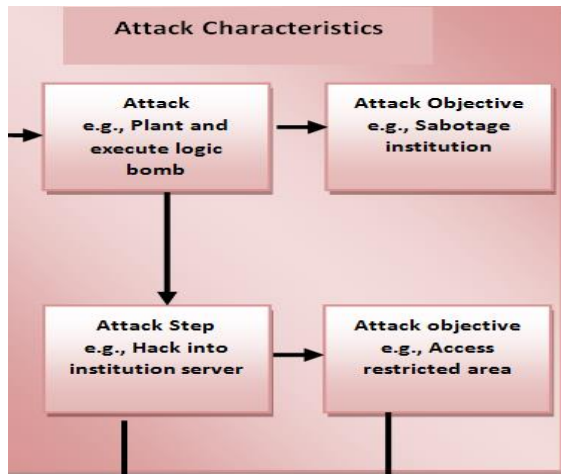
The last two elements of the model are the *resources*; they are the information systems with value to the organization and the interest of attack by the insider attacker. The second aspect is Vulnerabilities, which are the weakness in the assets or controls protecting them such as weak passwords, un-patched web servers and inadequate physical security among others. The model linked the vulnerability in the system such as management practices and technological protection techniques.



**Figure 3.7 Actor Element**

Source: (Nurse et al., 2014)

From the analysis of the elements, it is possible to bring together all of the elements of; precipitating events, personal traits, observed behavior, institution state and roles, targeted resources. With this model it is possible to characterize the insider the author presented their model as shown below figure



**Figure 3.8 Attack Element**

Source: (Nurse et al., 2014)

The nurse model presented above shows most the aspects of the model desired in a prediction model. It is also easy to implement since the elements in the model are based on existing theories in other disciplines such as psychology. The scholars in the research recommendations states that some of the elements makes the model difficult to implement hence need to look at how they can be made more lighter or activated for the model to work at any institution (Nurse et al., 2014).

### 2.8.5 Honeypot

Honeypot is a method used not only to detect the external attackers but can be used for internal attackers to trick them into making an attack on false information system in order to analyse the techniques that they use for the attack. The vulnerable systems are used to collect the methods and techniques that they use in attacking the system. The honeypot is an approach that was originally designed for detection of external threats but according Lance Spitzner, it can be used as an insider threat detector (Spitzner, 2003).

David Clock proposed honeypot as an external detection mechanism that was used to intercept attack and collect information about the behaviours of the attackers, tools and technique they used in attacking systems. Insider with malicious intent may be interested

with the ID, password, and confidential files among others. Configuration of honeypot is based on documents or e-mail such as confidential files and placed to the system. The insiders have access rights to access Honeypot, but this is not true. If the user accesses the Honeypot, it raises the question about the malicious intents of the user (Spitzner, 2003).

Honey model is best suited in cases where the institution would like to know how and where the system vulnerability lies and not as a predictive approach for the insiders. Therefore, it provides a good basis for updating a model but does not qualify as a model to be modified.

## **2.9 Literature Gap**

There are no a lot of data about insider security attack hence there are inadequate approaches of measuring the aspect of insider security threat. Mainly institutions that have been victims of insider security have concealed such cases because of the sensitive nature. Currently, most of the researches are still in progress on the prediction models and most of the insider security solutions in existence are based on research. However, the current security solutions presented are not satisfactory like the external security solutions. The problem with insider security solutions is that the insider has an information, access and skills together with understanding of the organizational structure with knowledge of internal system security. It is difficult to protect the internal resources using the approaches discussed in the above sections. It is very difficult to use the system administrators to protect internal resources. It is because the system administrators, who have access to all system resources are as well as insider security system, may have malicious intent. They are the biggest insider threat. This creates the need to look at a

model that is predictive. The model should not detect what has already been done but be able to tell us what is likely to take place and be able to secure the systems before it happens.

## **CHAPTER THREE**

### **RESEARCH METHODOLOGY**

#### **3.0 Study Area**

The study focused on information systems in two selected public universities in Kenya. The university is an institution of higher learning where different courses are offered from different levels starting from diploma, undergraduate and post-graduate. In Kenya, universities are mainly categorized into public and private universities. The selected public universities are under the government management under the ministry of higher education.

#### **3.2 Research Design**

Research design is important because it tell the readers the approach used in collecting data and hence the findings of the study. This study used quantitative approach. One of the reasons for choosing quantitative design is that they provide an actual bottom-line or dollar amount of the associated costs making them appealing in terms of non-technical decision making processes (Creswell et al., 2003). Quantitative models designed for information security analysis are mostly specific to organizational contexts. In this case it was suitable in the context of selected public universities in Kenya. There was a need to generalize the research findings of the study to other selected public universities and even private universities (Creswell et al., 2003).

### 3.2.1 Study Units

**Table 4.1 Study Units**

	<b>Specific objective</b>	<b>Study population units</b>	<b>Measurable variables indicator</b>	<b>Research design</b>
1	Establish information systems security insider threat in selected public universities in Kenya	Information systems expert Decision makers (head of section/departments/faculty) Information systems users	Age Training level Unauthorized access to data	Descriptive
2	Evaluate security mechanism in place in selected public universities in Kenya	Network administrators ICT technicians Data/database administrators Information security experts	Physical security measures in place (door) Security software installed Hardware security mechanism	Correlation
3	update an insider system security attack prediction model for insider security threats	Design procedures (factors or threats of security systems from insiders) Updating the model Testing the model Data collection	Application of existing models Update Existing models	

**Source: Researcher (2016)**

### **3.3 Quantitative Approach**

The quantitative research approach is one that the researcher uses to post-positivist claims for the developing knowledge. It is a method that one uses the strategies of inquiry such as questionnaires, experiments and collects data using instruments that yields statistical data (Creswell, 2003). Although there is no hypothesis in the study to be tested, quantitative approach is largely referred to as hypothesis-testing research

### **3.4 Research Strategy**

The research strategy was a general plan of how the study was used to address the research questions of the research study. The study strategy presents the intention to collect data and consider the constraints that the researcher faced in accessing data, location, ethical issues and money (Thornhill *et al.*, 2003).

### **3.5 Sample Selection**

This section outlines the study population, sampling techniques, target population and sample population of the study and how it was accomplished.

#### **3.5.1 Study Population**

According to Coolican (2014) target population is the entire set of units that the questionnaire data was used to inference. It means that the target population is that which the final results was generalized and it is from the target population that the researcher gets the sample population. The target population for the study was the two selected public universities in Kenya. The university employees especially those with access to information systems were the main target of the study. Therefore, actual population in this study that was established and accessed was as follows: information systems users, information system security policy enforcers, ICT experts, and heads of departments.

The following two universities were explored more since they are the area of study. The University of Interest was University of Eldoret and Kibabii University. University of Eldoret is Chartered Public University is approximately 9 kilometre from Eldoret town. It is located along the Eldoret-Ziwa road in Uasin Gishu County. The university has nine schools and faculties and one satellite campus; the Eldoret town campus. The vision of the university is to be a premier university that is globally visible in knowledge generation and technological innovations. This makes the current study more relevant on technological innovation and security of the information systems. The mission is to provide high quality education and training, in Science, Agriculture and Technology that promotes networking, partnerships and linkages with other institutions and industry. The structure of this university is as per the schools and faculties of university of Eldoret include; School Agriculture and Biotechnology, Schools of Business and Management Sciences, School of economics, school of education, School of Engineering, School of Environmental Studies, School of Natural Resource Management and School of Science. The schools/faculties offer diploma, undergraduate masters and doctoral degree programs. The ICT services in the University are under ICT Directorate. The directorate coordinate the running of the information systems in the entire university. Under the leadership of the ICT director, they formulate the ICT policies, deploy them and monitor their use by the university staff. In 2013, the university deployed the Enterprise resource planning (ERP) which has been praised as most successful. They allocate resources to the university users both students and staff members. According to the end of year speech by Prof. Akenga, there were over 17,000 enrolled in University of Eldoret. There are over 1,500 employees at the University of Eldoret.



Kibabii University Chartered Public. It is just 7 kilometres from Bungoma Town along the Chwele road traces its root from Kibabii Teachers Training College Bungoma County. The college was converted to a university college in August 2011 and it was gazetted as a constituent college of Masinde Muliro University and Technology through the legal notice No. 115. The current population of the university is over 6,000 students with estimated 2,000 employees. The university vision is to be a global and dynamic University of excellence in Science, Technology and Innovation. The vision coincides with the study topic on issues to do with security of the information systems. Technology and innovation is process that involves the use technologies such as the information systems. Kibabii University is anchored on the mission to achieve excellence in generation, transmission and enhancement of new knowledge in Science, Technology and Innovation through quality Teaching, Research, Training, Scholarship, Consultancy and Outreach programmes as per the university website.

### **3.5.2 Sampling Technique**

The elements of sampling are to have part of the population drawn to represent the entire population. Stratified random sampling was used to get the representation of the two strata of Kibabii University and University of Eldoret. The technique is more suitable since it reduces the sampling error and improves the representation of the sample (Hair *et al.*, 2010). Simple random sampling was used after stratification of the sample to get proportionate representation of each stratum.

### 3.5.3 Sample Size

The size of the sample determines the statistical accuracy of the findings. The sample size is a function of change in the population parameters being, it estimates the quality required by the researcher (Wegner, 2000). The sample size for the study was based on statistical table as provided by Krejcie and Morgan (1970), (Appendix B). The formula for determining sample size as presented is given as:

$$s = \frac{X^2 NP(1-P)}{d^2(N-1) + X^2 P(1-P)}$$

Where:

s –sample size desired

N=the population size

P= the population proportion (assumed to be 0.50 since it will give maximum sample size)

d = the degree of accuracy expressed as a proportion (0.05)

#### 3.5.3.1 Determination of the Population

The population sample was obtained from the people who use information as indicated in the study units based on the research objectives. The population represents the numbers from Kibabii University and University of Eldoret.

**Table 4.2 Sample Size of Information System Experts and Users**

<b>Role or title of respondents</b>	<b>Population (N)</b>	<b>Sample size (n)</b>	<b>Confidence level</b>
Information systems expert	45	41	95%
Information systems users	260	155	95%

Total	305	196	95%
-------	-----	-----	-----

**Source: Researcher (2016)**

### **Information systems experts**

$$X^2 NP(1-P) \div d^2(N-1) + X^2 P(1-P)$$

At 95% confidence level table value of  $X^2$  from the Chi-Square at df -1 table is 3.84

**(1.96<sup>2</sup>)**

$$N=45 \quad P=0.5 \quad d=0.05$$

$$3.84 * 45 * 0.5(1-0.5) \div 0.05^2(45-1) + 3.84 * 0.5(1-0.5)$$

$$= 43.2 / 1.07 = 40.4 \quad \sim = 41$$

### **Sample size for information system user population of 260**

$$X^2 NP(1-P) \div d^2(N-1) + X^2 P(1-P)$$

$$X^2 = 3.84 \quad (\text{table value of } 1.96)$$

$$N = 260 \quad P = 0.5 \quad d = 0.05$$

$$3.84 * 260 * 0.5(1-0.5) \div 0.05^2(260-1) + 3.84 * 0.5(1-0.05)$$

$$249.6 / (0.6475 + 0.96)$$

$$= 249.6 / 1.6075 = 155.272 \quad \sim = 156$$

### **3.6 Data Collection Instruments**

There are two main techniques to collection of data about problem, situation or phenomenon. Sometimes the data the researcher is looking for is available and only needs

extraction. There are other situations such as the current study where data must be collected (Hair *et al.*, 2003).

### **3.6.1 Questionnaire**

In this study quantitative questionnaire was used as an instrument of data gathering. Since the aim of the study was to establish the mechanisms in place for insider security threat. There were two sets of questionnaire; one for the system users and the other for the information systems experts (Appendix A). The questionnaires were designed based on the research objective and the information each group was expected to contribute to the study. A questionnaire is an approach was used to gather primary data from information system users.

### **3.6.2 Data Collection Procedures**

The introduction letter for data collection was obtained from Kisii University used for the introduction of the researcher to the institution authorities and the respondents. The researcher acquired a permit to carry out research from the National Council of Science and Technology (NACOSTI). The introduction letter and the research permit were presented to the selected universities who granted permission to carry out study in their institutions. The questionnaires were given to the respondents in person. The researcher used a drop and pick later approach for the questionnaires. The method was used to overcome time and costs limitations. The letters and permits acquired (Appendix D) are attached.

### **3.7 Quality Control**

Reliability and validity are two concepts that one must focus on when it comes to coming up with correct data and answers to the research questions on the research design (Saunders *et al.*, 2003).

### **3.7.1 Validity**

The reality of the results as they appear is referred to as validity of the results (Saunders *et al.*, 2003). Validity defined as the level at which data collection method or methods accurately measure what they were intended to measure (Saunders *et al.*, 2003). Cooper and Schindler (2003) believe that validity refers to the level at which a test measures what we actually wish to measure. Numbers of different steps were taken to ensure the validity of the study: The sources of data collection were reliable sources, from the respondents who actually use the information systems of the institutions and are in charge of securing the information systems; questionnaire questions were designed based on literature review to ensure the validity of the result; questionnaires were tested using pilot test before the start of the actual questionnaire and data was collected through a short period of two weeks which ensures no major events would take place to render data collected as invalid.

### **3.7.2 Reliability**

According to Saunders *et al.* (2003), reliability is the level to which data collection method will result into the consistent findings, similar observations would be realized or conclusions made by other investigators or there is transparency in the way data was collected from the field. SPSS software provides *Reliability Analysis Statistics*. The purpose of reliability test is for testing of the measurement of scales and the items it measures. Statistics: descriptive for every variable and the scale, inter-item correlations and covariance, ANOVA tables and reliability estimates were used in the study. Alpha Cronbach's test also was done has insider security mechanisms the results were tested and interpreted where a value more than 0.8 shows that there is strong reliability of the questions.

### **3.7.3 Pilot Test**

The purpose of a pilot test was to detect any weaknesses in the design and instrumentation and offer sample data. It was a process that simulated the procedures and steps that are put in place to be implemented during the actual processes (Cooper and Schindler, 2003). In this study, pilot test was carried. This exercise was aimed at eliminating ambiguity and improves on the quality of the data that was collected. The pilot study was carried out with the help of students doing masters at Kisii University. They were easily accessible and they are information systems experts hence their input was valuable and relevant for the study. Through the experts, the research questions were reviewed to bring out the study objectives. The students in this class composed of system users and information systems experts.

### **3.8 Data Analysis**

After data collection is completed, data analysis was the next step. To summarize and organize the data several procedures are performed during the data analysis stage (Zikmund, 2000). For quantitative data analysis, statistical tools of Microsoft excel and SPSS were used for data input and analysis. The statistical results were presented in graphical and tabular form with description. IBM Statistics (Version 21) was used by the researcher to analyse the data that collected.

### **3.9 Ethical Consideration**

The research ethical approach to study included the elements of responsibilities to participants, voluntary consent to give information, right to withdraw from the process, and ethical record keeping (BERA, 2011). The research ethical consideration was observed in the process of identifying, requesting for and collection of data from the respondents. Letters and permission were sought from relevant authorities. Only willing

respondents participated in the exercise without undue pressure. It means that those who were not willing were not be forced or coerced in taking the questionnaire. The names or any identification details of the respondents were not required for the respondents to take the questionnaire. All of the views expressed by the respondents were used only for the academic research only and not published for any other purposes.

## **CHAPTER FOUR**

### **DATA ANALYSIS AND INTERPRETATION**

#### **4.0 Introduction**

The purpose of this study was to establish insider security threats detection mechanisms and develops a model for detection of insider security system threats in selected public universities in Kenya. It further examined the gender, age and general knowledge of information systems users in relation to adhering to the security policy in place, the years of experience of the IT experts, the level of education, special training on ICT security on how they affect the systems security enforcement of the experts. There were three fundamental objectives that drove the collection of data and subsequent analysis. The objective of establishing the insider threats for information systems that universities face, the mechanisms put in place to deal with the insider threats and the third objective was to come up with a framework for detection of insider threats.

#### **4.1. Response Rate**

The study had two sets of sample population, the information systems experts and the information system users. The researcher got back 65 responses that is 82% representation of the feedback from the sample population. There were 4 questionnaires that were rejected and could not be used in the final work because they contained a lot of missing data or the respondents gave their personal details on the questionnaires hence could not be used for the study. The analysis for information systems users used 61 responses from the two universities.



**Table 5.1 The Rate of Response for Sample Population**

	<b>Information systems experts</b>	<b>Information systems users</b>	<b>Total</b>
Target Sample size	41	155	196
Realized	29	103	132
Rate of response (%)	70	66	67

(Source: Researcher 2016)

According to Williams (2014), the above response rates are acceptable since they are above 50% hence data analysis was done based on the response. There were 29 responses from experts while 103 were information systems users. The data was coded into two data sets for information systems experts and information systems users since they had different sets of questions.

#### **4.2 Missing Value**

This section carried out analysis to establish the missing values from the data. It was an essential exercise in the study because respondents who have never witnessed insider threat incident were not allowed to continue answering the questions. The responses with large number of missing values were excluded from the analysis. The missing variables were coded with value 9 to represent data that was missing in SPSS.

#### **4.3 Reliability and Validity Tests**

This section presents reliability test.

### 4.3.1 Cronbach Alpha Coefficients

The test of reliability is carried out using the Cronbach's test as tabulated below.

**Table 5.2 Reliability Test**

<b>Reliability Statistics</b>	
Cronbach's Alpha	N of Items
.905	7

The above table shows the test of reliability with the reliability statistics where 7 items were tested and the results shows a value of 0.905 which very high which indicates that there is a strong consistency among the seven motivations for insider attack items.

The study also tested to establish the effect if one of the items from the seven motivations of insider attackers was removed on the reliability of the other items. The results are tabulated below in table below.

**Table 5.3 Scale Mean if Item Deleted**

<b>Item-Total Statistics</b>		
	Scale Mean if Item Deleted	Cronbach's Alpha if Item Deleted
Attackers are motivated by financial gain	17.1000	.869
Attackers are motivated by disgruntlement	16.6500	.871
Attackers are motivated by revenge	17.0500	.899
Attackers are motivated by getting attention	16.6000	.902
Attackers are motivated by no reward	17.1500	.929
Attackers are motivated by no promotion	16.8500	.867
Attackers are motivated by espionage	17.4000	.884

From the above table, it is only attackers motivated by no reward item that would increase the level of overall reliability if it was deleted from a value of .916 to .929.

Removing either revenge as motivation and getting attention does not significantly lower

the reliability of the items. However, the motivations of insider attackers as financial gain, disgruntlement, no promotion and espionage if either one of them is removed lowers the internal consistency of the items below .902 but not lower than .867 which is still an acceptable level of reliability in social science.

#### 4.4 Tests for Assumptions of Normality

The study used of Kolmogorov-Smirnov (K-S) and the Shapiro-Wilk (S-W) for the tests of the assumption that the study data are drawn from a normally-distributed population. The two tests were used because the data is interval data. The two tests were done to test the null hypothesis that all data come from a normally-distributed population. Therefore, alternate hypothesis is that data come from a population that is not normally distributed. The use of the two tests was to validate each other. The significant tests for p is less than 0.05( $p < 0.05$ ) for accepting the null hypothesis. The test for normality is important for other statistics such as ANOVA which make assumption that data is normally distributed.

**Table 5.4 Tests of Normality**

		Tests of Normality					
		Kolmogorov-Smirnov <sup>a</sup>			Shapiro-Wilk		
Gender of Respondents		Statistic	df	Sig.	Statistic	df	Sig.
Attackers are motivated by	Male	.204	15	.093	.860	15	.024
Financial Gain	Female	.235	7	.200*	.856	7	.139
Attackers are motivated by	Male	.245	15	.016	.836	15	.011
disgruntlement	Female	.236	7	.200*	.806	7	.047
Attackers are motivated by	Male	.250	15	.012	.823	15	.007
Revenge	Female	.241	7	.200*	.937	7	.609
Attackers are motivated by	Male	.172	15	.200*	.925	15	.230
espionage	Female	.267	7	.140	.894	7	.294

\*. This is a lower bound of the true significance.

a. Lilliefors Significance Correction

The test for normality distribution was carried out on three variables, which were seeking the opinion of the respondents on motivation of the insiders attacking the information systems. They were factored by gender for male and female. The statistics for Kolmogorov Smirnov shows the value greater than 0.05 apart from only two variables; the motivation of disgruntlement and revenge as factor by male is less than 0.05. Shapiro-Wilk gives similar results with additional of motivation of financial gain for male. Based on the above statistics visual analysis of the variable to establish if the null hypothesis can be accepted or rejected should be done.

#### **4.5 Security Threats in the Universities**

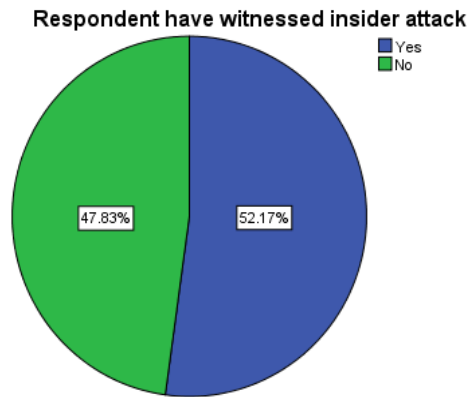
##### **4.5.1 Establish Insider Threats in Selected public universities in Kenya**

This section addressed the first research question on the insider security threats that selected public universities are facing today. The researcher sought to establish if universities have been a victim of insider security attack or the vulnerability of the systems that exposes the system to threats.

###### **4.5.1.1 Witnessed or Probed the Insider Security Incidences**

The statistics in this section seeks to establish if there has been any. The experts and the information systems users were asked if they had witnessed heard or probed insider security attacks. Most of the respondents at 79% stated that they had witnessed it in the current work station. However, there were 20% of the respondents who said that they had not witnessed, probed or encountered insider security attacker in the current work station.

#### 4.5.1.2 Experts Witnessed or Aware of Insider Attack Incident



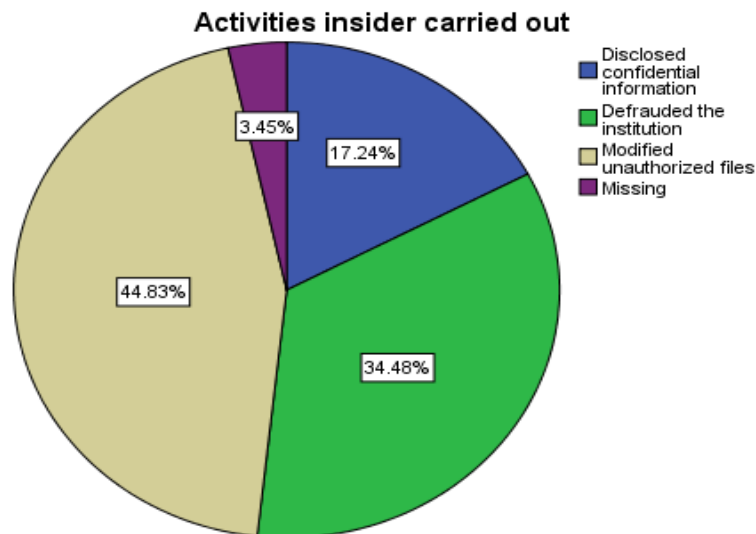
**Figure 5.1 Users Witnessed or Aware of Insider Attack Incident**

The pie chart above shows results of the information system users on whether they have witnessed, heard or probed insider attack in the university particularly in their departments or sections. Slightly more than half of the respondents (52%) said that they have come across the incident but 48% said they had not.

Based on the results from the information systems experts and the information systems users, it is clear that insider security attacks do occur or have happened in the selected public universities. The first research question is addressed by more than 50% in each category of those that stated they have witnessed, experienced or even been victim of insider security threat.

#### 4.5.1.3 Activities Carried Out

The study further sought to establish some of the activities that the insiders carried out.



**Figure 5.2 Activities Carried Out**

The study sought to find out some of the activities that insider attackers carried out. Most of the insider attackers targeted modification of files in the system. The study established that about 45% stated that the activities carried out were modification of files that they had no authorization of modifying. The study further established that about 34% of the attackers carried out activities that defrauded the institution. In this case they were after financial gain. However, about 17% that disclosed the confidential information.

#### 4.5.2 How the Respondents Know the Insider Attacker Incidents

The question sought to establish how information on incident of the insider attacker in the institution.

##### 4.5.2.1 Heard or Know About Insider Incident

**Table 5.5 How they Heard or Knew About Insider Incident**

	Frequency	Percent	Valid Percent	Cumulative Percent
Department Meeting	5	17.2	22.7	22.7
Involved in Investigation	7	24.1	31.8	54.5
Valid From Colleagues	6	20.7	27.3	81.8
University Reports	4	13.8	18.2	100.0
Total	22	75.9	100.0	
Missing 9.00	7	24.1		
Total	29	100.0		

The above table shows the means of how they get information on the insider incidents on those who said they had witnessed, heard or aware of insider incidents in the university. 27% of the respondents stated that they become aware from friends while most of the respondents are people involved in the investigation of the insider incidents at 31% it is worth noting that university reports was listed as the least means of knowing that insider incident has occurred at 18%. The results excludes those who said they did not know of any insider incident.

#### 4.5.2.2 Action Taken Against Insiders

The study sought to find out about the actions that those who were found to be the insiders in the institutions and the results are presented in the table below.

**Table 5.6 Action Taken Against the Insider Attacker**

	Frequency	Percent	Valid Percent	Cumulative Percent
Insider Terminated	4	13.8	18.2	18.2
Suspended and forced to resign	6	20.7	27.3	45.5
Valid Demoted	9	31.0	40.9	86.4
Transferred to other department	3	10.3	13.6	100.0
Total	22	75.9	100.0	
Missing 9.00	7	24.1		
Total	29	100.0		

The frequency table above shows that most of the individual found to have attacked the system and they have access to it was demoted at 41% while 27% of the culprits were suspended and forced to resign. There was no reporting of the case to the police as per responses from the experts. There was 24% missing which are linked to most who said they never heard, probed or witnessed insider security threat.



#### 4.5.2.3 Activities Carried Out

The study sought from experts on this that the insider had done. The results are presented in the table below;

**Table 5.7 Activities Carried Out or Aim of the Attacker**

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Disclosed confidential information	6	20.7	27.3	27.3
Valid Defrauded the institution	6	20.7	27.3	54.5
Valid Modified files they had no authentication	10	34.5	45.5	100.0
Valid Total	22	75.9	100.0	
Missing 9.00	7	24.1		
Total	29	100.0		

The results show that 46% of the insider incidents involved illegal modification of files. There were 27% of the respondents who said they either disclosed confidential information and same score said they defrauded the institution. It indicates that most of the cases in the public university targeted access to files that the users did not have access.

#### 4.5.2.4 Damage Causes as a Result of Insider Activities

The study sought to establish the damages that insider threats caused to the university system when they occurred. The results are presented in the table below;

**Table 5.8 Damage Was Done/Effects of the Insider Activities**

	Frequency	Percent	Valid Percent	Cumulative Percent
Defrauded the University	8	26.7	27.6	27.6
Valid Services Stopped	16	53.3	55.2	82.8
Deleted Files	5	16.7	17.2	100.0
Total	29	96.7	100.0	
Missing System	1	3.3		
Total	30	100.0		

The frequency table above shows that 55% of the incidents resulted to services stopping at the university. It means that things were not running normally and essential services were not being offered. 27% of the respondents said that insider incidents result to loss of money (defrauded the university) with about 17% stating that files were deleted during the incidents.

#### 4.6 Mechanisms in Place in Universities Against Insiders

The objective was to examine the current mechanisms that the university has put in place to control insider security threats. Since it is evident that selected public universities have experienced insider security breaches, it is essential to establish the measures in place in dealing with the insider threats. The literature identified several mechanisms that are being used in other institutions to counter insider security threats; the study divided the measures into technology, personnel and procedures or processes. The respondents were asked to what extent they agree or disagree with the statements on some of the practices

and mechanisms in place for security measures against insiders. There were elements dropped after pilot study and the remaining elements are in the questionnaire for information system users from question 6-18

**Table 5.9 KMO and Bartlett's Test**

<b>KMO and Bartlett's Test</b>		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.709
Bartlett's Test of Sphericity	Approx. Chi-Square	607.148
	Df	66
	Sig.	.000

The Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy was carried out and it indicates the proportion of variance in the variables that might be caused by the underlying factors. The KMO value for instruments was 0.709, which was acceptable as the middling value (Kaiser, 1974). Additionally, Bartlett's test of sphericity tests for the hypothesis that the correlation matrix is an identity matrix was done. The test was significant which means that the variables are unrelated and therefore unsuitable for structure detection. The Bartlett's test shows that there is statistical significant level hence the variables were accepted for further study.

#### 4.6.1 Factor Analysis

**Table 5.10 Total Variance Explained**

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.452	28.764	28.764	3.452	28.764	28.764	3.229	26.912	26.912
2	1.512	12.596	41.360	1.512	12.596	41.360	1.493	12.442	39.354
3	1.317	10.973	52.333	1.317	10.973	52.333	1.435	11.955	51.309
4	1.130	9.420	61.753	1.130	9.420	61.753	1.204	10.035	61.344
5	1.035	8.629	70.382	1.035	8.629	70.382	1.085	9.039	70.382
6	.805	6.710	77.092						
7	.710	5.913	83.005						
8	.678	5.650	88.656						
9	.536	4.469	93.125						
10	.455	3.793	96.918						
11	.274	2.283	99.201						
12	.096	.799	100.000						

Extraction Method: Principal Component Analysis.

Factor analysis was carried out to extract various mechanisms that are being used in guarding against insider security threats in selected public universities. The method of extraction was Principal Component Analysis. Kaiser recommends that factors with eigenvalues greater than 1 should be retained. Five factors with eigenvalues greater than 1 were extracted and it accounts for about 70% of the variability in the original variables. The table above shows the factors that were extracted, factor loading and rotation factors presented.

**Table 5.11 Factor Loading for Mechanisms Against Insider Security**

<b>Rotated Component Matrix<sup>a</sup></b>					
	Component				
	1	2	3	4	5
Trained by the university on security protection methods for information systems	.927	.052	-.030	-.031	.081
Trained regarding password strength, complexity and scheduled changes?	.823	-.067	-.093	-.173	-.081
Strong and mandatory password change after a period of time	.726	-.158	.061	.025	.146
Frequency of change your password	-.217	.594	-.386	-.182	-.126
Give sensitive or confidential digital information to county or state regulators without proper authorization	.023	-.169	.710	.060	.208
Discuss or disclose sensitive or confidential digital information during personal conversations while at work	-.506	.564	-.067	.224	.156
Discuss or disclose sensitive or confidential information with non-employees while away from work	-.042	-.085	-.015	.908	-.030
You aware of methods external system attackers can get confidential digital information from you	-.913	.101	.046	-.201	-.026
The university trained you how to recognize a legitimate warning message	.071	.039	.106	-.005	.902
I manually lock your computers when you are away from your desks	.026	.799	.102	-.082	.016
The institution allow you to install programs on the university computers	.130	-.044	-.652	.390	.016
Institution has a well-accepted "Bring Your Own Device" policy in place	-.055	.320	.560	.250	-.388
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.					
a. Rotation converged in 7 iterations.					

The table above is the rotated matrix table using Varimax with Kaiser Normalization. It gives how individual factor relates with the component. The component with values higher than 0.6 are regarded as with high relationship with the component since variance

is high. The score is measure from 0 to 1 where scores close to 0 are weak relations and those close to 1 shows strong correlation.

**Table 5.12 Factor and Mechanism used in Public University**

Factor	Item	Factor loading	Mechanism name
1	Trained by the university on security protection methods for information systems	0.927	Information Security awareness
	Trained regarding password strength, complexity and scheduled changes?	0.823	
	strong and mandatory password change after a period of time	0.726	
2	Discuss or disclose sensitive or confidential digital information during personal conversations while at work	0.564	Manage organizational culture
	I manually lock your computers when you are away from your desks	0.799	
	you aware of methods external system attackers can get confidential digital information from you	0.101	
	Frequency of change your password	0.594	
3	Institution has a well-accepted "bring your own device" policy in place	0.560	Information Security policy
	Give sensitive or confidential digital information to county or state regulators without proper authorization	0.710	
4	Discuss or disclose sensitive or confidential information with non-employees while away from work	0.908	Access control and authentication
	The institution allow you to install programs on the university computers	0.390	
5	The university trained you how to recognize a legitimate warning message	0.902	Physical access control

The literature groups the security mechanisms into informal, formal and technical mechanism. The grouping below shows that selected public universities use a combine of the mechanisms as categorized below.

**(a) Security awareness-** security awareness or education is often seen as one of the mechanism that institutions use is protecting the systems. Training of the information users on security protection methods, trained regarding password strength and strong and mandatory password change. The factors are training of employees on the methods of protecting the information systems and the need of having a strong and period change of password.

**(b) Manage organizational culture-** this is a mechanism that is aimed at having a culture which protects the information and related resources. Ensuring that information users do not disclose information while away from work and having a policy on how users can access critical resources are key mechanisms captured as factors in the above table.

**(c) Security policy-** there is a security policy in place for protection of the information systems. It is a mechanism that can be used in against insider security attackers. The factors in this mechanism are disclosure of confidential digital information during personal conversations and installation of programs on university computers. If the information system can install programs then they have administrative rights and it can affect the security of the information system.

**(d) Authentication and access control-** the two mechanisms have been combined although in literature they are explored separately. Training on password strength and recognizing legitimate warning message are part of access control while manually lock of the computer access control mechanism.

(e) **Physical access control-** remote access is accessing the systems away from the university premises and giving information to regulators without authorization is about physical access control mechanism.

#### 4.7 Motivators of Insider Security Threat

In order to come up with insider security model, it is important to understand the motivators of insider security threat. Both the information systems experts and the information systems users were surveyed on the possible motivators for trusted person in the public university to breach information systems security policy.

##### 4.5.1 Insider Attackers are Motivated by Financial Gains

**Table 5.13 Insider attackers are Motivated by Financial Gains**

<b>Insider attackers are motivated by Financial Gains</b>					
		<b>System experts</b>		<b>System Users</b>	
		Frequency	Percent	Frequency	Percent
Valid	Strongly Agree	15	50.0	73	45.3
	Agree	9	30.0	54	33.5
	Not Sure	3	10.0	1	.6
	Disagree	2	6.7	33	20.5
	Total	29	96.7	161	100.0
Missing System		1	3.3		
Total		30	100.0		

The table above shows the frequency results of the information experts and users when asked about financial gain being the motivator for insider attackers about 80% of both users and experts of the information systems agreed that financial gain is the reason for



insider attackers. There were 10% of the experts who said they were not sure but 20% of the users felt that financial gain was not a motive.

#### 4.7.2 Insider Attackers are Motivated by Disgruntlement

**Table 5.14 Insider Attackers are Motivated by Disgruntlement**

Insider attackers are motivated by Disgruntlement					
		System experts		System Users	
		Frequency	Percent	Frequency	Percent
Valid	Strongly Agree	6	20.0	79	49.1
	Agree	14	46.7	48	29.8
	Not Sure	5	16.7	31	19.3
	Disagree	4	13.3	2	1.2
	Total	29	96.7	1	.6
Missing	System	1	3.3	161	100.0
Total		30	100.0		

The frequency table shows the responses for the information system users and experts on the statement that insider attackers are motivated by disgruntlement. 67% of the expert users said that insiders are disgruntled while about 79% of the information users had the same view. About 17% and 19% of the system experts and systems users were not sure about disgruntlement as the motive for attackers. Based on the responses above there is agreement among the users and experts that insiders who are disgruntled pose a security threat to the organization.

#### 4.7.3 Insider Attackers are Motivated by Revenge

**Table 5.15 Insider Attackers are Motivated by Revenge**

<b>Insider attackers are motivated by Revenge</b>					
		Systems experts		System users	
		Frequency	Percent	Frequency	Percent
Valid	Strongly Agree	12	40.0	89	55.3
	Agree	9	30.0	69	42.9
	Not Sure	4	13.3	3	1.9
	Disagree	4	13.3		
	Total	29	96.7	161	100.0
Missing	System	1	3.3		
Total		30	100.0		

Revenge as per the literature was found to be a motivator of insider attackers. The responses from the information systems highly support this opinion with about 97% agreement that revenge drives insiders to pose as threats. However, information systems experts were divided on this statement with 70% agreeing that revenge is a motivator but 13% remained neutral with similar score disagreeing with the statement. Revenge is seen as a strong motivator among the systems users as well as systems experts.

#### 4.7.4 Insider Attackers are Motivated by Getting Attention

**Table 5.16 Insider Attackers are Motivated by Getting Attention**

<b>Insider attackers are motivated by getting attention</b>					
		System experts		System users	
		Frequency	Percent	Frequency	Percent
Valid	Strongly Agree	1	3.3	15	9.3
	Agree	7	23.3	35	21.7
	Not Sure	8	26.7	39	24.2
	Disagree	9	30.0	72	44.7
	Strongly Disagree	4	13.3		
	Total	29	96.7	161	100.0
Missing	System	1	3.3		
Total		30	100.0		

The frequency table above shows that most of the information systems experts and users felt that insider attackers are not motivated by seeking attention. 26% of the experts and 31% of the users agreed that they seek attention. However, 44% of the systems users and 43% of the experts disagreed with the statement that insider attackers are motivated by seeking attention from the management or other colleagues.

#### 4.7.5 Insider Attackers are Motivated by Not Rewarded

**Table 5.17 Insider attackers are Motivated by not Rewarded**

		System Experts		System Users	
		Frequency	Percent	Frequency	Percent
Valid	Strongly Agree	4	13.3	3	1.9
	Agree	11	36.7	113	70.2
	Not Sure	5	16.7	32	19.9
	Disagree	4	13.3	13	8.1
	Strongly Disagree	5	16.7		
	Total	29	96.7	161	100.0
Missing System		1	3.3		
Total		30	100.0		

The above table shows results of the systems experts and system users on the statement that insider attackers are motivated by lack of reward. 49% of expert and 72% of the information users agreed that lack of reward is likely to drive an insider to become hostile to the information system and the information system security policy. 29% of the experts did not agree with the statement. It suggests that most of the information users agree compared to information system experts. It should be noted that about 20% of the experts were not sure if this is a motivator.

#### 4.7.6 Insider Attackers are Motivated by Lack of Promotion

**Table 5.18 Insider Attackers are Motivated by Lack of Promotion**

		Frequency	Percent	Frequency	Percent
Valid	Strongly Agree	10	33.3	39	24.2
	Agree	10	33.3	92	57.1
	Not Sure	2	6.7	1	.6
	Disagree	7	23.3	29	18.0
	Total	29	96.7	161	100.0
Missing System	1	3.3			
Total	30	100.0			

67% of the information systems experts agreed the statement that insider attackers are motivated by lack of promotion. The statement was also agreed at 81% of the information systems experts. 23% of experts disagreed as well as 18% of users with the statement that insiders are motivated by lack of promotion to attack the system.

#### 4.7.7. Insider Attackers are Motivated by Espionage

**Table 5.19 Insider Attackers are Motivated by Espionage**

		Frequency	Percent	Frequency	Percent
Valid	Strongly Agree	1	3.3	38	23.6
	Agree	10	33.3	91	56.5
	Not Sure	6	20.0	3	1.9
	Disagree	8	26.7	29	18.0
	Strongly Disagree	4	13.3		
	Total	29	96.7	161	100.0
Missing System	1	3.3			
Total	30	100.0			

Espionage in literature was seen as greatest motivator among corporates on trade secrets, the study sought to find out if it is also a motivator in selected public universities. The experts did not think that espionage was a motivator with 39% disagreement and further 20% remaining neutral on the issue. However, over 80% of the information systems users were of the opinion that espionage was the reason for insider attackers. It suggests that experts and users had differences in opinion on the issue of espionage for the insider threat.

#### **4.8 Summary**

The chapter has presented the results analysis for the study based on the objectives. There were two sets of data; for information systems experts and information systems users. The study findings show that selected public universities have insider security incidences where respondents stated they have experienced witnessed or probed insider threat incidents. The independent variables of the study are; human, physical and system risks. Through factor analysis, the study has explored each variable on how they affect the security of the system. The analysis established that human factors are not being taken into consideration by the selected public universities because training of the information users and organization culture factors were not being implemented. The universities do not report in official reports the insider incidents where most respondents hear about it during staff meeting when they are briefed to probe while others hear from colleagues. The study further establishes that there are several factors that make it possible for the insiders to successfully execute malicious activities. These are the intervening variables of the study conceptual framework. About the motivators of insider attack, the study concludes that all motivators are present apart from seeking attention by the attackers. The dependent variables of the study were tested. Loss of integrity of data, fraud and theft of intellectual property were witness as a result of insider attackers. Modification of the files was the main activities in the incidences where insider attackers modified files they were not authorized to alter.

## **CHAPTER FIVE**

### **DISCUSSION AND CONCLUSION**

#### **5.0 Introduction**

The research sought to establish detection strategies for malicious insiders in selected public universities in Kenya. The intent of this study was to collect data that facilitated a comprehensive analysis and development of insider threat detection and mitigation framework for selected public universities. This section presents the summary of the findings of the study, discussions in relation to the literature and the conceptual model and updating an insider system security attack prediction model.

#### **5.1 Discussion**

The role that staff and other players have in the organization is paramount despite the technological advancement. It means that organization including the academic institutions need information systems to be able to accomplish different tasks. The discussions are structured as per the research objectives.

#### **Objective one: Establish information systems security insider threats in selected public universities in Kenya**

The study established that 79 per cent of the information experts and 52 per cent of the information systems experts have heard, probed, or witnessed insider security incidences in their current work stations. There were more experts aware of the insider incidents by the fact that they have access to information on security issues of the systems unlike the information users. Similarly Abomhara & Kjøien (2015), states that insiders can pass crucial information to the outside attacker hence they are a threat. The findings further agree with what Liu et al., (2018), established that there is an increased trend of security breaches coming from people trusted by companies. They further state that there is need



to have methods of detecting and preventing insider cyber security threats. However more than half of the users said they are aware of the incidents because they are at senior management level as dean of schools/faculties or as heads of departments. Most of the insider attackers targeted modification of files in the system. The study established that about 45% stated that the activities carried out were modification of files that they had no authorization of modifying. Magklaras & Furnell (2001) had similar findings although they were looking at different environment from the institution of higher learning. They established that misuse of IT resources was cited as the most common activity of the insider attackers. According to the report by Carnegie Mellon University in 2012 concluded that large amount of information security threats are posed by people known and very trusted by the institution they are affiliated with. The level of damage or the activities of the attackers as per the study was mainly to defraud the institution, modify data and disclose the confidential information of the system. U.S Secret Service, the CERT insider Threat Center, CSO Magazine and Deloitte study concluded that 46 percent of the insider attackers were serious attacks than what the external attacks could have caused. The study further stated that having a model to predict the attack could have reduced the incidents. It showed that insider attacks if successfully can by 46 percent more severe than external attackers because there are not insider attack prediction models like in external systems. Silowash *et al.* (2012), attributes the severity of the attack by insiders to the fact that they are trusted and have authorized access to the systems resources hence easy to expose or steal intellectual property is easy.

The research findings agree with what Njoroge (2013) established in her study. The study by Njoroge (2013) while looking at post implementation factors for information

systems security concluded that end users at 75 percent contributed to the security of the system. The findings were also similar to what Nyamongo (2012) found. In her study although attributed security breaches to information systems users at about 48 percent for user errors and compromising of information systems at 45 per cent. The study at 79 percent by the information systems experts and 52 percent by the information systems pointed out that they have encountered insider security threats. Information system users (insiders) are major contributors of the information systems security threats. The current study presents findings that are in agreement with those of scholars in literature (Schultz, 2002, Nyamongo 2012; Claycomb *et al.*, 2012; Njoroge 2013; Nostro, 2014 and Boender *et al.*, 2014).

**Objective two: Evaluate insider system security mechanism in place in selected public universities in Kenya**

According to Nyamongo (2012) in her study on security management in private chartered universities in Kenya, pointed out that universities are ready and willing to have security mechanisms in place to counter the security incidents. The study also established that there are efforts in place in the university to deal with insider security threats. Similarly, the study established that there are efforts in place to deal with insider security threats. Selected public universities are carrying out: security awareness or education is often seen as one of the mechanism that institutions use is protecting the systems. Training of the information users on security protection methods, trained regarding password strength and strong and mandatory password change. The findings are in a agreement with what Wang, Liu & Zhang (2006), concluded in their study as they were establishing prediction model. They further add that security awareness on mechanisms of preventing insider

attacker should be carried out on regular basis. The factors are training of employees on the methods of protecting the information systems and the need of having a strong and period change of password. The technical report by Team (2013) points to unintentional insider threats points out to failure of the organization to create awareness on methods that insider attackers can use to other credentials of other employees. Aspects such as organizational culture were cited by the report as source of unintentional insider threats. Organizational systems culture, this is a mechanism that is aimed at having a culture which protects the information and related resources. Samnani, Salamon & Singh (2014), points to negative effect of the workplace behavior in security management that agrees with organizational culture aspects. They agree with the study findings that ensuring that information users do not disclose information while away from work and having a policy on how users can access critical resources are key mechanisms captured. Security policy, there is a security policy in place for protection of the information systems. It is a mechanism that can be used in against insider security attackers. Additionally, there are Authentication and access control where training on password strength and recognizing legitimate warning message are part of access control while manually lock of the computer access control mechanism and physical access control. Remote access is accessing the systems away from the university premises which Spitzner (2003) found to be security threat for insiders as giving information to regulators on authorization compromises physical access control mechanism. The study established that only information security awareness and information security policy have been enhanced in selected public universities. Nyamongo (2012) pointed out that universities have not established a specific information system security department to deal with security

management of the university. The university does not have centralized way of dealing with the issues of information security.

Daniel (2008), recommends that business strategies and plans should be put in place to mitigate the insider security threats. The existing intrusion taxonomies are descriptive of the attacks and are not designed to particularly monitor insider misuse. 63 percent of the respondents were of the opinion that selected public universities in Kenya have business continuity plan that addresses the backup and recovery of vital information systems in case of an insider attack or any type of attacker. It is a positive step but there is need to test and reconfigure the plan to meet the complexity that insider attackers present and dynamic business environment.

### **Objective three: Updating an insider system security attack prediction model for insider security threats**

This objective was based on the study literature on current models and the study findings. The study explored some of the motivators of insider threats so as they can be incorporated in the model. Both users and experts of the information systems were surveyed on this question and the results showed greater agreement on the motivators of financial gain, lack of reward, lack promotion, disgruntlement and revenge as motivators. The motivators were established in the studies of Wood (2000); Theoharidou et al., (2005); Qutaibah & Panda (2008); Santos et al., (2008); Nurse, et al., (2014) Rauthmann et al., 2015 and Liu et al., 2018. However, some studies such Rauthmann et al., 2015 disagreed that seeking attention was a significant motivator for insiders to attack which can relate to the study where small number saw this as a motivator. However, there was

significant differences in the view of the experts on espionage as a motivator as to the views of the system users. Experts said it was not a motivator while most of the system users felt it was a great motivator. After the researcher made follow-up to several system users on their response, it was evident that most were not familiar with the term espionage. Therefore, better results could have been attained with a simpler term to the system users. In this regard, the views of the experts were taken into considerations since Hunker (2011), had established espionage as significant motivator. Espionage has been established as also a motive of insider attacks in the study. The insider is used by the attackers outside the organization as leverage to facilitate theft of information (Claycomb *et al.*, 2012). In most cases, criminals entice employees into perpetrating attacks without even the employees knowing. There are cases where multiple motivators occur at once where the insider is motivated by financial gain but also felt that they did not get fair promotion. After a search on his home computers, letters offering to sell secrets to Libya, China and Iraq was revealed. In respect to Iraq, the perpetrator had asked Saddam Hussein regime for \$13 million (Magklaras & Furnell, 2001). Investigation revealed that the specialist not only he been motivated by monetary gains, but also a sense of disgruntlement as he constantly complained to his co-workers and neighbours about his job and station.

Financial gain was a motivator of insider security with 47 percent of the attacks in the university had been traced to financial gain. According to FBI/CSI, 10 percent of the financial losses as a result of electronic crime was as a result of insiders in 2001 which increased to 23.7 percent of the loss in 2006. The survey report further revealed that out of the \$52,494,290 loss as a result of information security attacks, \$12,466,810 was

attributed to insiders in 2006 which is 13.7 percent increase between 2001 and 2006. According to studies conducted by USSNTAC and CSEI, 81% of the insider threats were motivated by financial gains.

## **5.2 Conclusion**

The study sought to determine if there were cases of insider threats for the information systems in selected public universities. It further set out to evaluate the methods or mechanisms that are being used by the universities in protecting the university information systems against the insiders. The last objective was to come up with a prediction model that universities can use in preventing occurrences of the insider threats. The study used two selected public universities in accomplishing the objectives. The results show that universities have had cases of insiders. The targets are modification of unauthorized information in the computer, fraud and exposing the system to external attackers. *Therefore, the study concludes that selected public universities in Kenya face insider security threats.* The universities have put in physical, management and logical controls to secure the systems. However, the measures are best suited for external attackers of the system than the internal attackers. This is because they have all the credentials to pass through the security check and even access to information systems. The detection systems in place in the selected public universities only report cases that have already taken place. Therefore, there is no model that can be used to predict the insider security. The study concluded that there are increased cases of insider attacks in selected public universities in Kenya. The motives of attacks vary but they are not specific for each university as per the research findings. It is critical that a model should be formulated to predict the behaviour of the insiders before they attack the system.

## **CHAPTER SIX**

### **RECOMMENDATION**

#### **6.0 Introduction**

The study recommends the use of a predictive model to prevent more insider security incidents. The study further proposes a model to use for insider security threats prediction. The model by (Nurse *et al.*, 2014) for prediction is recommended. However, the study recommends modification on the model to fit the academic institution. The areas of the model to be modified are presented.

#### **6.1 Proposed Insider Detection Model**

The proposed model for predicting the insider attacks was realized out of the need for a precise and better prediction model where different components of the insider threat issue could be easily understood and implemented. The study was guided by the research objective and the scope of the creation of the framework. Based on the study finding, the *motivation to attack* that describes the reasons that made an individual to attack their institution. The element of motivation was analyzed in the study together with the relevant literature that narrowed down the number of key motivators to insider attackers.

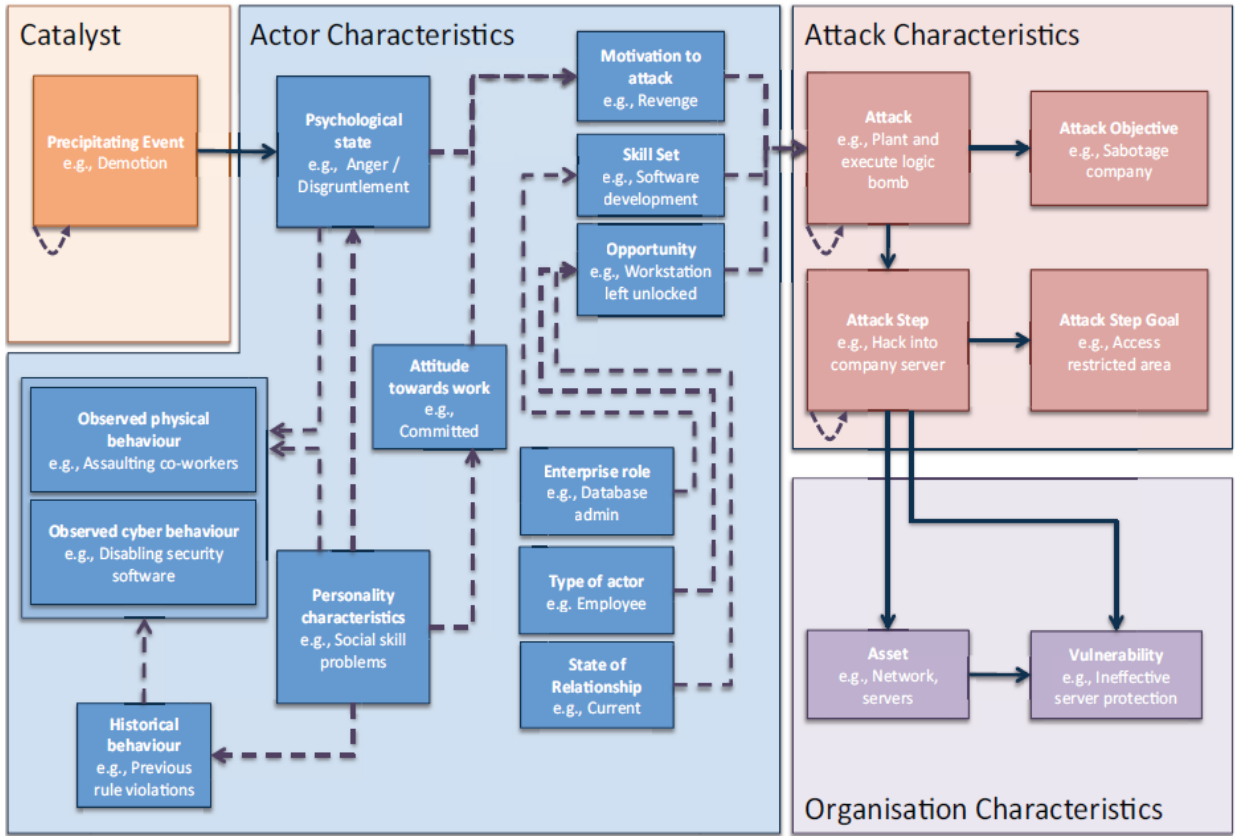
After reviewing several models, the model by Nurse *et al.* (2014), with minimal modifications meets the solution for prediction of insider security threats in universities in Kenya as per the study findings. It is also the most recent model that captures aspects from other older models with new perspectives.

Nurse *et al.* (2014), captures the most important indicators that can be used by the universities to predict insider threats. The model by the Nurse *et al.* (2014), presents some challenges, the scholars have also acknowledged in their limitations. The study also observed the same challenges such as getting background information of the employees

from previous companies or the criminal investigation department. The study findings show that universities do not have pre-screening functions. Additionally, most of the information systems users are not required to have certificate of good conduct. The study further established that individual probed as insiders are not reported to the police where actions such as inter-department transfers, demotion are more common for the culprits. Therefore, the police do not have records help in declining to issue certificate of good conduct. Selected public universities depend on referees in screening new employees which is not reliable since many organizations do not report on insider activities. Measuring the psychological behavior and the mind-set of the attackers in organization requires specialized personal like a psychologists or specialized HR personnel. This dynamic element of the model makes it difficult to act on some of the activities hence making the model ineffective. The dynamic traits are very complicated and difficult to map to the model. The study proposes elimination of the dynamic traits since they are not only difficult to identify and map on the model but they make the model ineffective. Eliminating the model element from the framework for public university model for insider security threat prediction makes it more effective.



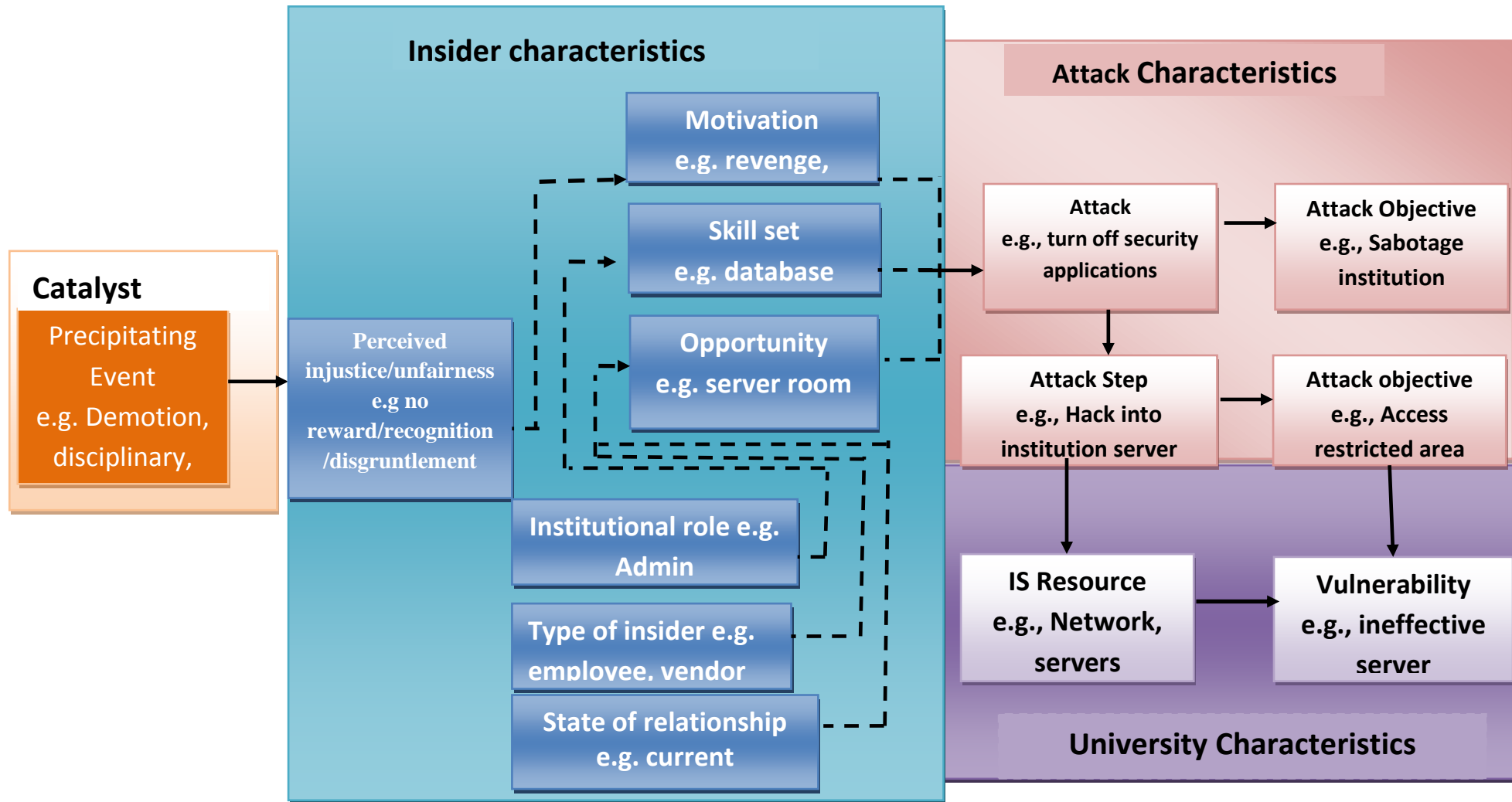
### 6.1.1 The Elements Recommended for Removal in Next Model



**Figure 7.1 Insider Attack Prediction Model By Nurse and Others**

Source (Nurse *et al.*, 2014)

### 6.1.2 Recommended Model



Source: (Researcher, 2016)

Figure 7.2 A Model for Predicting Insider Attacks

### **6.1.3 The elements of the model**

The model presented in **Error! Reference source not found.** is made up of several elements. The elements represent four areas; *the motivator* henceforth referred to as *catalyst*, *insider characteristics*, attack characteristics and the institution characteristics. The insider as defined in the study will hence forth be referred to as actor. Specific elements are represented by the use of boxes while the solid arrows indicate the relation between elements with dashed lines indicating the potential associations (Nurse *et al.*, (2014). The study has further broken down the model into sections with the aim of simplifying the discussion and implementation of the model. The main sections of the models are; understanding the motivation to attack; dissecting the attack, the resources (information systems) under attack and their vulnerabilities.

#### **Precipitating event (Catalyst)**

They are the catalyst that has an influence on the insider which can tip them to become threats of the information system. As per the literature the participating events are referred to as ‘tipping point’ (Moore *et al.* 2008). They are events such as employee dismissal, employee disciplinary actions, disputes with other employees, perceived injustices, company actions such as lay-offs, personal problems such as divorce, health related issues among others, new opportunities like getting a better paying job in another company. The study largely based the human factors on participating events from the research in the area of Counterproductive Workplace Behaviour (CWB) (Samnani, Salamon & Singh, 2014) where events such as lack of promotion, inadequate or no rewards for committed employees and financial gain were evaluated on the study area. It was established that most of the attacks witnessed

in the selected public universities were tipped off or triggered by at least one of the participating factors.

A significant aspect that was evident from the study was that most of the attacks were based on perception or rumours of something bad that was about to happen as indicated established by (Wallnau, 2013). Similar studies (Samnani, Salamon & Singh, 2014; Schneier, 1999) where system administrators starting to create a logic bomb based on rumours reducing allowances is an example. The precipitating event elements are wide, this need to be appreciated as there are many aspects that can trigger an employee to an insider attacker.

## **6.2 Validation of the Insider Detection Model**

Validation of the recommended model is important for theoretical and practical purposes. The model presented gives the prediction ability to the information systems of the Universities in Kenya against insider threats. As per Yin (1994) validity of the model is about the relevance and meaningfulness of the model. There are five aspects that should be used in measuring the validity of a model as suggested by Pederson *et al.* (2000): truth, internal logic, acceptance, applicability and novelty value. The internal logic and the truth are about the basis of the results of the study which is based on existing theories; there should be a link between the starting point, research questions of the study and the final study outcome. It is the exploitation of the practical results to be used and the theoretical applications in explaining the phenomena.

There are two methods used for validation of the research findings and the recommended insider threat detection model. To start with, the data collection method used for the study was validated. The study used pilot study and the actual research study where the final outcome was validated by the pilot study results. Additionally,

statistical test on validity of the study was carried out where a strong validity for the items was recorded. Closed ended questionnaire with likert scale was used to get the responses. The data was used to come up with a model that had all the key variables to the model tested. The research results formed the basis of coming up with the recommended model. Secondly, the researcher presented the model to the experts in information systems who were the supervisors. Since the model is a modification of already existing model the experts explored the critical success factors of the model without aspects dropped from the original model. It was further fine-tuned from the feedback to the current final model as recommended.

## REFERENCES

- Abomhara, M., & Kjøien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security*, 4(1), 65-88.
- Baker, W.H., Hylender, C.D. & Valentine, J.A. (2008). *2008 Data Breach Investigations Report*. Obtained from [www.verizonbusiness.com](http://www.verizonbusiness.com), October 2008.
- Baracaldo, N., & Joshi, J. (2012). A trust-and-risk aware rbac framework: tackling insider threat. In *Proceedings of the 17th ACM symposium on Access Control Models and Technologies* (pp. 167-176). ACM.
- Bellovin, S.M. (2008). *The Insider Attack Problem Nature and Scope*. In Stolfo, S.J. et al. *Insider Attack and Cyber Security, Beyond the hacker*, New York, Springer Science, pp. 1-4.
- British Educational Research Association. BERA (2011). *The role of research in teacher education: Reviewing the evidence*.
- Bishop, M. (2013). *Panel: The Insider Problem Revisited*. In Proceedings of the 2005 workshop on New security paradigms (Lake Arrowhead, USA), pp. 75-76.
- Bishop, M., Conboy, H. M., Phan, H., Simidchieva, B., Avrunin, G. S., Clarke, L., ... & Peisert, S. (2014). Insider Threat Identification by Process Analysis. In *Security and Privacy Workshops (SPW), 2014 IEEE*(pp. 251-264). IEEE.
- Boender, J., Ivanova, M. G., Kammuller, F., & Primiero, G. (2014). Modeling human behaviour with higher order logic: insider threats. In *Socio-Technical Aspects in Security and Trust (STAST), 2014 Workshop on* (pp. 31-39). IEEE.
- Bojanc, R., Jerman-Blazic, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management* 28, pp. 413-422.

- Brackney, R.C., Anderson, R.H. (2004). *Understanding the Insider Threat*. In Proceedings of a March 2004 Workshop (March 2-4, 2004, Rockville, MD, USA).
- Brdiczka, O., Liu, J., Price, B., Shen, J., Patil, A., Chow, R., ... & Ducheneaut, N. (2012). Proactive insider threat detection through graph learning and psychological context. In *Security and Privacy Workshops (SPW), 2012 IEEE Symposium on* (pp. 142-149). IEEE.
- Butts, J.W., Mills, R.F. & Baldwin, R.O. (2005). *Developing an Insider Threat Model Using Functional Decomposition*. In Proceedings of the Third international workshop on mathematical methods, models, and architectures for computer network security (St. Petersburg, Russia, September 25-27), pp. 412-417.
- Capelli, D., Moore, A., Shimeall, T.J., Trzeciak, R. (2009). *Common Sense Guide to Prevention and Detection of Insider Threats v3*. Obtained from [http://www.cert.org/insider\\_threat/](http://www.cert.org/insider_threat/), January 2009.
- Caliendo, M., Fossen, F., & Kritikos, A. S. (2014). Personality characteristics and the decisions to become and stay self-employed. *Small Business Economics*, 42(4), 787-814.
- Carroll, M.D. (2006). *Information Security: Examining and Managing the insider Threat*. In Proceedings of the 3rd annual conference on Information security curriculum development, Kennesaw, Georgia (USA).
- Carroll, T. E., Greitzer, F. L., & Roberts, A. D. (2014). Security informatics research challenges for mitigating cyber friendly fire. *Security Informatics*, 3(1), 13.
- Claycomb, W. R., Huth, C. L., Flynn, L., McIntire, D. M., Lewellen, T. B., & Center, C. I. T. (2012). Chronological examination of insider threat sabotage: preliminary observations. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 3(4), 4-20.

- Coolican, H. (2014). *Research methods and statistics in psychology*. Psychology Press.
- Cummings, A., Lewellen, T., McIntire, D., Moore, A. P., & Trzeciak, R. (2012). *Insider threat study: Illicit cyber activity involving fraud in the US financial services sector* (No. CMU/SEI-2012-SR-004). CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.
- Crawford, M., & Peterson, G. (2013, January). Insider Threat Detection using Virtual Machine Introspection. In *System Sciences (HICSS), 2013 46th Hawaii International Conference on* (pp. 1821-1830). IEEE.
- Creswell, J. W., Plano Clark, V. L., Gutmann, M. L., & Hanson, W. E. (2003). Advanced mixed methods research designs. *Handbook of mixed methods in social and behavioral research*, 209, 240.
- Daft, R.L. (2000). *Management*. Harcourt College Publishers, Orlando, USA. 5th edition, pp.670.
- Dhillon, G. (2001). Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns. *Computers & Security* 20 (2), pp.165-172.
- Dhillon, G., Moores, S. (2001). Computer crimes: theorizing about the enemy within. *Computers & Security* 20 (8), pp.715-723.
- Ezingard, J. N., Mcfadzean, E., & Birchall, D. (2005). A model of Information Assurance Benefits. *Information Systems Management* 22 (2), pp. 20-29.
- Gritzalis, D., Stavrou, V., Kandias, M., & Stergiopoulos, G. (2014, March). Insider Threat: Enhancing BPM through Social Media. In *New Technologies, Mobility and Security (NTMS), 2014 6th International Conference on* (pp. 1-6). IEEE.
- Gunasekhar, T., Rao, K. T., & Basu, M. T. (2015, March). Understanding insider attack problem and scope in cloud. In *Circuit, Power and Computing Technologies (ICCPCT), 2015 International Conference on* (pp. 1-6). IEEE.



- Herrmann, D. S. (2002). *Using the Common Criteria for IT Security Evaluation*. CRC Press.
- Hunker J, Probst, C (2011) Insiders and Insider Threats An Overview of Definitions and Mitigation Techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 2(1), 4-27
- Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, 1(1), 80.
- Inness, M., Barling, J., & Turner, N. (2005). Understanding supervisor-targeted aggression: a within-person, between-jobs design. *Journal of Applied Psychology*, 90(4), 731.
- ISO/IEC 15408 (1999). Information technology — Security techniques — Evaluation criteria for IT security. ISO/IEC Switzerland.
- Keromytis, (2008). *Hard Problems and Research Challenges Concluding Remarks*. In Stolfo, S.J. *et al.* Insider Attack and Cyber Security, Beyond the hacker, New York, Springer Science, pp. 215-218.
- James F. Broder, G. T. (2011). *Risk Analysis and the Security Survey*. Elsevier.
- Janes, P (2012) Information Assurance And Security Integrative Project People, Process, And Technologies Impact On Information Data Loss. [Online] Available at: <http://www.sans.org/reading-room/whitepapers/dlp/people-process-technologies-impact-information-data-loss-34032> [Accessed 15 May 2016]
- Kandias, M., Virvilis, N., & Gritzalis, D. (2013). The insider threat in Cloud computing. In *Critical Information Infrastructure Security* (pp. 93-103). Springer Berlin Heidelberg.
- Kizza, J. M. (2009). *A guide to computer network security*. Springer.

- Kammüller, F., Nurse, J. R., & Probst, C. W. (2016). Attack tree analysis for insider threats on the IoT using Isabelle. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 234-246). Springer, Cham.
- Liebald B., D. R. (2012). *Proactive Detection Of cyber attacks*.
- Liu, L., De Vel, O., Han, Q. L., Zhang, J., & Xiang, Y. (2018). Detecting and Preventing Cyber Insider Threats: A Survey. *IEEE Communications Surveys & Tutorials*, 20(2), 1397-1417.
- Magklaras, G. B., & Furnell, S. M. (2001). Insider threat prediction tool: Evaluating the probability of IT misuse. *Computers & Security*, 21(1), 62-73.
- Magklaras G, Furnell S, ( 2005) A preliminary model of end user sophistication for insider threat prediction in IT systems. *Computers & Security*, 24 (5), 371-80.
- Mick, J. (2010, August 28). USB Stick Led to Worst Cyber Attack on U.S. Military; Russia Suspected. *DailyTech* .
- Micki Krause Nozaki, H. F. (2011). *Information Security Management Handbook, Sixth Edition, Volume 5*. CRC Press.
- Montes-y-Gómez, M., Gelbukh, A., and López-López, A. (2000). Comparison of Conceptual Graphs. In *Proceeding of MICA-2000, In 1st Mexican International Conference on Artificial Intelligence*
- Moore, A. P., Cappelli, D. M., & Trzeciak, R. F. (2008). The “big picture” of insider IT sabotage across US critical infrastructures. In *Insider Attack and Cyber Security* (pp. 17-52). Springer US.
- Nguyen, H.; Santos, E Jr.; Zhao, Q.; and Wang, H. (2004b). Capturing User Intent for Information Retrieval. *Proceedings of the 48th Annual Meeting for the Human Factors and Ergonomics Society (HFES-04)*, new Orleans, LA. Pages 371- 375

- Njoroge, G. W. (2013). Factors Influencing post Implementation System Security of Management Information Systems: A Case Study of Nairobi City Water and Sewerage Company, Nairobi County, Kenya. Nairobi, Nairobi, Kenya.
- Nostro, N., Ceccarelli, A., Bondavalli, A., & Brancati, F. (2014). Insider threat assessment: A model-based methodology. *ACM SIGOPS Operating Systems Review*, 48(2), 3-12.
- Nurse, J. R., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R., & Whitty, M. (2014). Understanding insider threat: A framework for characterising attacks. In *Security and Privacy Workshops (SPW), 2014 IEEE* (pp. 214-228). IEEE.
- Nozaki, Y. (2015). Emotional competence and extrinsic emotion regulation directed toward an ostracized person. *Emotion*, 15(6), 763.
- Olsen, L., & Zaman, M. (2013). Insider trading and motivations for earnings management. *Journal of Accounting and Finance*, 13(3), 51-66.
- Qutaibah A., & Panda, B. (2008) Performance analysis of an insider threat mitigation model. ICDIM: 703- 709
- Rauthmann, J. F., Sherman, R. A., Nave, C. S., & Funder, D. C. (2015). Personality-driven situation experience, contact, and construal: How people's personality traits predict characteristics of their situations in daily life. *Journal of Research in Personality*, 55, 98-111.
- Samnani, A. K., Salamon, S. D., & Singh, P. (2014). Negative affect and counterproductive workplace behavior: The moderating role of moral disengagement and gender. *Journal of Business ethics*, 119(2), 235-244.
- Santos, E , Nguyen, H.; Zhao, Q. & Wang, H (2003a). User modelling for intent prediction in information analysis. Proceedings of the 47th Annual Meeting for the Human Factors and Ergonomics Society. Pages 1034–1038.

- Santos, E, Nguyen, H, Yu, F, Kim, K, Li, D, Wilkinson, J, Olson, A, Jacob, R (2008): Intent-driven Insider Threat Detection in Intelligence Analyses. 2008 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology, 2008.
- Schneier, B (1999) Attack trees: Modeling security threats. *Dr. Dobb's Journal*, December 1999.
- Spitzner, L (2003). Honeypots: Catching the Insider Threat, 19th Annual Computer Security Applications Conference (ACSAC '03)
- Stavrou, V., Kandias, M., Karoulas, G., & Gritzalis, D. (2014). Business Process Modeling for Insider threat monitoring and handling. In *Trust, Privacy, and Security in Digital Business* (pp. 119-131). Springer International Publishing.
- Sterman, J. D. (2006). Learning from evidence in a complex world. *American journal of public health*, 96(3), 505-514.
- Team, C. I. T. (2013). Unintentional insider threats: A foundational study. *Software Engineering Institute Technical Report*.
- Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security*, 24(6), 472-484.
- Wallnau, K. (2013). *Engineering Realistic Synthetic Insider Threat (Cyber-Social) Test Data*. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.
- Wang, H, Liu, S, & Zhang, I (2006). A Prediction Model of Insider Threat Based on Multi-agent. 2006 1<sup>st</sup> International Symposium on Pervasive Computing and Applications.
- Williams, A. (2014). How to... Write and analyse a questionnaire. *Journal of Orthodontics*.

Wood, B. (2000). An insider threat model for adversary simulation. *SRI International, Research on Mitigating the Insider Threat to Information Systems*, 2, 1-3.

## **PPENDICES**

### **APPENDIX A**

#### **Questionnaires**

##### **a. Information Systems Experts**

###### **PART A: PEOPLE**

1. What is name of university you work?  
 Kibabii University  University of Eldoret
2. Which of the following professions/department do you work under? (mark the suitable box)  
  
 Computer and Information security Systems Manager  
  
 Web Administrator/ Webmaster  
  
 Network System Administrator  
  
 Database Administrator
3. How long have you been working for your current institution?
  - (a) 0 - 1 year
  - (b) 1 – 2 years
  - (c) 3 – 4 years
  - (d) 4 years or more
4. Are you motivated in the workplace?
  - i. Do you feel that the organization is rewarding you as per your efforts?  
Yes  No
  - ii. When was the last time you got a promotion?  
12 months  2 years  3 years  4 years or more
  - iii. Were your colleagues happy about it?  
Yes  Not sure  No  Some
5. Have you ever heard/witnessed/suspected/probed insider attacks in your professional life?

Yes

No

*Please answer the following by marking the appropriate box.*

6. Insiders might assist external parties such as terrorists, foreign states, business competitors among others intentionally or unknowingly. Have you ever come across such issues?

Yes

No

a) What activity did the person do?

Disclosed confidential information  Defrauded the institution

Modified authorized files

b) Insider attackers are motivated by:

	Strongly Agree (SA)	Agree (A)	Not Sure (N)	Disagree (D) And Strongly Disagree (SD)	Strongly Agree (SA)
financial gains					
Disgruntlement					
Revenge					
Get attention					
They feel not well rewarded					
Lack of promotion/salary increment					
Espionage					

c) What level was the insider trusted within the organization. Tick as indicated in the table below.

	Strongly un-trusted	Not trusted	Neither trusted nor	Trusted	Strongly trusted
Your view on level of trust					

accorded to the insider					
----------------------------	--	--	--	--	--

7. What damage was caused?

Operations brought to a halt  Property stolen money lost

Customer information lost  Patents & copy rights

8. Prior to the attack, the insider was in good terms with superiors

Strongly Agree  Agree  Not Sure  Disagree  Strongly Disagree

9. Prior to the attack the insider raised any issues with the organization that in their opinion could have been addressed

Strongly Agree  Agree  Not Sure  Disagree  Strongly Disagree

10. The university conducts security awareness activities as part of security management best practices

Strongly Agree  Agree  Not Sure  Disagree  Strongly Disagree

(a) The security awareness is effective in terms of employee adherence and satisfaction

Strongly Agree  Agree  Not Sure  Disagree  Strongly Disagree

(b) Some employees resent [respondent negatively] the such processes

Strongly Agree  Agree  Not Sure  Disagree  Strongly Disagree

(c) The training was carried out after Incidences of insider attacks were reported

Strongly Agree  Agree  Not Sure  Disagree  Strongly Disagree



## PART B: PROCESSES

Access control processes in an organization limit events, actions and conditions within an IT system.

1. The university has a security policy and can be accessed on any information  

Strongly Agree  Agree  Not Sure  Disagree  Strongly Disagree
2. There are physical and electronic access controls in place in the university to ensure security of the organization, its property and workers  

Strongly Agree  Agree  Not Sure  Disagree  Strongly Disagree
- How often, for example, do you change your password?  

once per month  after three months  After six months  after a year  never changed password
3. The university uses access control policies to restrict access to privileged individuals only?  

Strongly Agree  Agree  Not Sure  Disagree  Strongly Disagree
4. Employees are allowed extended privileges such as accessing networks and systems from remote locations  

Strongly Agree  Agree  Not Sure  Disagree  Strongly Disagree
5. The IT department is responsible for creation and deletion of employee accounts upon employment or termination of a new employee the institution  

Strongly Agree  Agree  Not Sure  Disagree  Strongly Disagree
6. Employees account are immediately deleted or deactivated once they are termination or exit of the employee?  

Strongly Agree  Agree  Not Sure  Disagree  Strongly Disagree
7. There is a laid down strategy of deactivating an employee account and it is not done at the discretion of the system and network administrators?  

Strongly Agree  Agree  Not Sure  Disagree  Strongly Disagree

**PART C: TECHNOLOGY**

1. As an employee, I am allowed to bring and use your own devices in the workplace  
such as phones, Laptops, USB sticks, external memory etc.

Strongly Agree [ ] Agree [ ] Not Sure [ ] Disagree [ ] Strongly Disagree

2. The university has special conditions that authorize the use such devices in the course  
of your duty

Strongly Agree [ ] Agree [ ] Not Sure [ ] Disagree [ ] Strongly Disagree

3. I would check on institution systems if you were to find a USB stick left at your desk  
or along the way or in the corridor

Strongly Agree [ ] Agree [ ] Not Sure [ ] Disagree [ ] Strongly Disagree

4. There is no any technological methods applied by your organization to combat insider  
attacks

Strongly Agree [ ] Agree [ ] Not Sure [ ] Disagree [ ] Strongly Disagree

5. The university is doing all it can to combat insider threats

Strongly Agree [ ] Agree [ ] Not Sure [ ] Disagree [ ] Strongly Disagree

6. The strategies being utilized to combat insider threats are effective

Strongly Agree [ ] Agree [ ] Not Sure [ ] Disagree [ ] Strongly Disagree

7. What in your opinion is the leading cause of insider threats?

Reasons for insider threats	Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
Lack of Policy					
Weak organizational policies					
unsatisfied employees					
ineffective technology					
Lack of awareness					

8. The organization has a Business Continuity or Disaster Recovery Plan?

Strongly Agree [ ] Agree [ ] Not Sure [ ] Disagree [ ] Strongly Disagree

9. The university has business Continuity Plan cover backup and recovery procedures for all virtual systems?

Strongly Agree [ ] Agree [ ] Not Sure [ ] Disagree [ ] Strongly Disagree

10. The vendors provide other services in addition to security testing?

Strongly Agree [ ] Agree [ ] Not Sure [ ] Disagree [ ] Strongly Disagree

11. The university uses a local Intrusion Detection System(s) (IDS)?

Strongly Agree [ ] Agree [ ] Not Sure [ ] Disagree [ ] Strongly Disagree

12. If your university uses local IDS, do you use

“host-based” IDS (HIDS) [ ]

“network-based” IDS (NIDS) [ ] or

a combination of both [ ]

13. Any other information that you deem relevant, comment, or remark.

.....  
.....  
.....

**NOTE:**

**PRIVACY CLAUSE**

All the information collected in this questionnaire is exclusively used for the purposes of this research and cannot be shared with any third party whatsoever.

Your cooperation and support will be highly appreciated.

Signed: \_\_\_\_\_

Date: \_\_\_\_\_

**b. Employees/Information System Users**

**Employee/system user of public university in Kenya**

Dear Respondent

I am a student pursuing MSc. Information Security Systems. I am writing a thesis on; *Modofying a Security Model for Detection of Insider Security Systems Threats in Selected public universities in Kenya.*

Insider attacks are such a huge security threat in organizations today. They are as a result of intentional or accidental misuse by persons authorized to access and use information systems. In most instances, insiders manipulate existing security controls, ensuring that they are least detected, and finally instituting massive losses.

An insider is a trusted person with full privileges and access rights to organizational systems and physical facilities. They may include present and past employees, contractors, partners and visitors. Insider attacks may occur due to a number of factors including espionage, and motive of disgruntlement, criminal financial gains or revenge.

Kindly assist by taking a few minutes of your time to answer my questionnaire about your personal experience with insider threats within and beyond your organization

Your opinion will be highly appreciated.

Thanks for your anticipated cooperation.

1. Kindly indicate your gender

Male  Female

2. How long have you worked in the current workstation?

1-3  3-5  5- 8  8-10 years  more than 10 years

3. Kindly indicate your position

Faculty/school Dean  COD/HOD  assistant Admin  Head of Section   
support Staff

4. Have you heard/encountered misuse of information system resources like disclosure of digital files or give access to unauthorized person?

Yes  No

5. An employee may pose a threat for information systems if they have the following motives

	Strongly Agree (SA)	Agree (A)	Not Sure (N)	Disagree (D)	Strongly Disagree (SD)
Disgruntlement					
Revenge					
Get attention					
They feel not well rewarded					
Lack of promotion/salary increment					
Espionage					
financial gains					

6. I have been trained by the university on security protection methods for information systems

Strongly Agree  Agree  Not Sure  Disagree  Strongly Disagree

7. I Have been trained regarding password strength, complexity and scheduled changes

Strongly Agree  Agree  Not Sure  Disagree  Strongly Disagree

**8.** The organization enforces strong password procedures for employees, including requiring a mandatory password change after a period of time?

Strongly Agree  Agree  Not Sure  Disagree  Strongly Disagree

**9.** I often change my password

Strongly Agree  Agree  Not Sure  Disagree  Strongly Disagree

**10.** I can disclose digital information to county or state regulators without proper authorization?

Strongly Agree  Agree  Not Sure  Disagree  Strongly Disagree

**11.** I do discuss or disclose sensitive or confidential digital information during personal conversations while at work?

Strongly Agree  Agree  Not Sure  Disagree  Strongly Disagree

**12.** I do discuss or disclose sensitive or confidential information with non-employees while away from work

Strongly Agree  Agree  Not Sure  Disagree  Strongly Disagree

**13.** I am aware of methods external system attackers can get confidential digital information from you

Strongly Agree  Agree  Not Sure  Disagree  Strongly Disagree

**14.** The university has trained me how to recognize a legitimate warning message from a scam message that could result in downloading a virus

Strongly Agree  Agree  Not Sure  Disagree  Strongly Disagree

**15.** I manually lock my computers when I am away from my desks

Strongly Agree  Agree  Not Sure  Disagree  Strongly Disagree

**16.** Does the institution allow you to install programs on the university computers?

Yes  No

**17.** The institution has a well-accepted "Bring Your Own Device" policy in place

Strongly Agree [ ] Agree [ ] Not Sure [ ] Disagree [ ] Strongly Disagree

18. I can access university system [like ERP] while away from the university

Strongly Agree [ ] Agree [ ] Not Sure [ ] Disagree [ ] Strongly Disagree

19. Any other information that you deem relevant, comment, or remark.

.....  
.....  
.....

**NOTE: PRIVACY CLAUSE**

All the information collected in this questionnaire is exclusively used for the purposes of this research and cannot be shared with any third party whatsoever.

Signed: \_\_\_\_\_

Contact (feedback/follow purposes) \_\_\_\_\_

Date: \_\_\_\_\_

## APPENDIX B

### Statistical Table for Determining Sample Size

*Table for Determining Sample Size from a Given Population*

<i>N</i>	<i>S</i>	<i>N</i>	<i>S</i>	<i>N</i>	<i>S</i>
10	10	220	140	1200	291
15	14	230	144	1300	297
20	19	240	148	1400	302
25	24	250	152	1500	306
30	28	260	155	1600	310
35	32	270	159	1700	313
40	36	280	162	1800	317
45	40	290	165	1900	320
50	44	300	169	2000	322
55	48	320	175	2200	327
60	52	340	181	2400	331
65	56	360	186	2600	335
70	59	380	191	2800	338
75	63	400	196	3000	341
80	66	420	201	3500	346
85	70	440	205	4000	351
90	73	460	210	4500	354
95	76	480	214	5000	357
100	80	500	217	6000	361
110	86	550	226	7000	364
120	92	600	234	8000	367
130	97	650	242	9000	368
140	103	700	248	10000	370
150	108	750	254	15000	375
160	113	800	260	20000	377
170	118	850	265	30000	379
180	123	900	269	40000	380
190	127	950	274	50000	381
200	132	1000	278	75000	382
210	136	1100	285	100000	384

Note.—*N* is population size.  
*S* is sample size.

Source: Krejcie and Morgan (1970)



## **APPENDIX C**

### **Letters of Authorization and Permit**

The following are the letters and permits sought from different authorities in to enable the researcher carry out study.



# KISII UNIVERSITY

(ISO 9001:2008 Certified Institution)

**ELDORET CAMPUS**

**OFFICE OF THE DEPUTY DIRECTOR-ACADEMIC AFFAIRS**

Phone: 020-2610479

Email:eldoretcampus@kisiiuniversity.ac.ke

P. O. Box 408- 40200  
ELDORET-KENYA

2<sup>ND</sup> SEPTEMBER , 2016

TO WHOM IT MAY CONCERN

Dear Sir / Madam.

**RE: RESEARCH DATA COLLECTION PERMIT.**

**DENIS WALUMBE WAPUKHA      MIN11/20403/14**

The above named is a bonafide student of Kisii university- Eldoret Campus pursuing a **Master's Degree in Information Systems** in the faculty of **Information Science and Technology**.

He is working on his research entitled "*Designing a Security Model For Detection Of Insider Security Threats in Public Universities In Kenya*" in partial fulfilment for the requirement of the Award of Masters in **Information Systems**.

We are kindly requesting your office to provide him with the permit to proceed to the field for data collection and completion of his research.

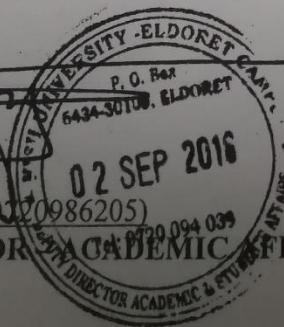
Please do not hesitate to call the undersigned for any verification.

Any assistance extended to him will be highly appreciated.

Yours faithfully,

Charles O. Ongiyo (01120986205)

**DEPUTY DIRECTOR-ACADEMIC AFFAIRS**



NACOSTI

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

Telephone: +254-20-2213471,  
2241349, 3310571, 2219420  
Fax: +254-20-318245, 318249  
Email: dg@nacosti.go.ke  
Website: www.nacosti.go.ke  
When replying Please quote

9th Floor, Utalii House  
Uhuru Highway  
P. O. Box 30623-00100  
NAIROBI-KENYA

Ref: No.

Date:

NACOSTI/P/16/69328/13625

28<sup>th</sup> September, 2016

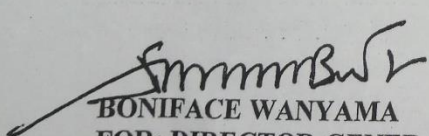
Denis Wapukha Walumbe  
Kisii University  
P.O. Box 402-40800  
KISII.

**RE: RESEARCH AUTHORIZATION**

Following your application for authority to carry out research on "*Designing a security model for detection of insider security systems threats in public universities in Kenya*," I am pleased to inform you that you have been authorized to undertake research in **Bungoma and Uasin Gishu Counties** for the period ending **28<sup>th</sup> September, 2017**.

You are advised to report to the **Vice Chancellors of selected universities, the County Commissioners and the County Directors of Education, Bungoma and Uasin Gishu Counties** before embarking on the research project.

On completion of the research, you are expected to submit **two hard copies and one soft copy in pdf** of the research report/thesis to our office.

  
BONIFACE WANYAMA  
FOR: DIRECTOR-GENERAL/CEO

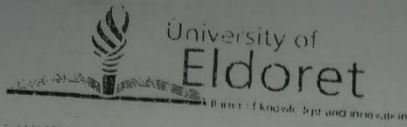
Copy to:

The Vice Chancellors  
Selected Universities.

The County Commissioner  
Bungoma County.







P. O. Box 1125 - 30100 Eldoret, Kenya  
Tel: +254 53 2063257 / 20 337123 Fax: 2352/3  
Mob: 0736 493557; Fax: 0254 53 206 3257  
E-mail: [dvasa@uod.ac.ke](mailto:dvasa@uod.ac.ke)  
Website: [www.uod.ac.ke](http://www.uod.ac.ke)

**OFFICE OF THE DEPUTY VICE-CHANCELLOR**  
**Academic & Students' Affairs**

Our Ref. UoE/B/DVASA/DRIV/034

Date: 21<sup>st</sup> March, 2017

Denis Walumbe Wapukha  
Kisii University - Eldoret Campus  
P. O. BOX 6434-30100,  
**ELDORET, KENYA**

Dear Mr. Wapukha,

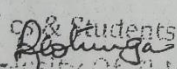
RE: PERMISSION TO COLLECT DATA FROM UNIVERSITY OF ELDORET

The above subject refers.

This is to inform you that your request to collect data for your Masters Research topic: *"Designing a security model for detection of insider security system treats in public universities in Kenya"* has been granted.

You will be required to report to Director of Research and Innovation for briefing on protocol adherence when carrying out research as stipulated in our policies. Kindly note that data collected shall be used for research purposes only.

Yours Sincerely,

  
PROF. RUTH N. OTUNGA  
DEPUTY VICE-CHANCELLOR  
ACADEMIC & STUDENTS' AFFAIRS

cc Director, Research & Innovation



**KIBABII UNIVERSITY**  
(Knowledge for Development)

Tel: 020 - 2028660 / 0708 - 085934 / 0734 - 831729  
P.O. Box 1699 - 50200  
Bungoma

E-mail: [enquiries@kibabiiuniversity.ac.ke](mailto:enquiries@kibabiiuniversity.ac.ke) /  
[vc@kibu.ac.ke](mailto:vc@kibu.ac.ke)  
Website <http://www.kibabiiuniversity.ac.ke>

**OFFICE OF THE DEPUTY REGISTRAR (ADMIN. & HR)**

**Our Ref. KIBU/ADM/CORR. 77/VOL.1/**

**Date: 23<sup>rd</sup> May, 2017**

TO WHOM IT MAY CONCERN

Dear Sir/Madam,

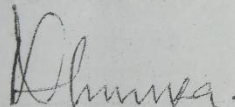
**RE: PERMISSION FOR RESEARCH DATA COLLECTION**

Mr. Dennis Wapukha Walumbe is a student of Kisii University pursuing Master's Degree in Information Systems in the Faculty of Information Science and Technology.

He has been granted permission to collect data from members of Kibabii University for his study titled '*Designing a Security Model for Detection of Insider Security Threats in Public Universities*'.

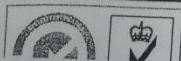
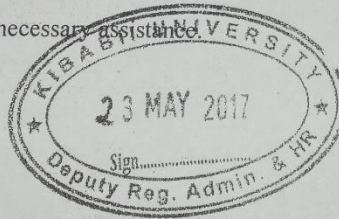
Kindly accord him any necessary assistance.

Yours faithfully,

  
David Butali Namasaka

**DEPUTY REGISTRAR (ADMINISTRATION AND HUMAN RESOURCES)**

Copy to: DVC (PPRI)  
Security Officer II



**Kibabii University ISO 9001:2008 Certified**



## AN UPDATE TO THE INSIDER SYSTEM SECURITY ATTACK PREDICTION MODEL TO SUIT SELECTED PUBLIC UNIVERSITIES IN KENYA

### ORIGINALITY REPORT

<b>12%</b>	<b>9%</b>	<b>4%</b>	<b>7%</b>
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

### PRIMARY SOURCES

<b>1</b>	<b>Submitted to Nottingham Trent University</b> Student Paper	<b>1%</b>
<b>2</b>	<b>mafiadoc.com</b> Internet Source	<b>1%</b>
<b>3</b>	<b>Jaeseung Hong, Jongwung Kim, Jeonghun Cho. "Chapter 13 The Trend of the Security Research for the Insider Cyber Threat", Springer Science and Business Media LLC, 2009</b> Publication	<b>1%</b>
<b>4</b>	<b>Submitted to Laureate Higher Education Group</b> Student Paper	<b>1%</b>
<b>5</b>	<b>wwwhome.cs.utwente.nl</b> Internet Source	<b>&lt;1%</b>
<b>6</b>	<b>hdl.handle.net</b> Internet Source	<b>&lt;1%</b>
<b>7</b>	<b>repository.mua.ac.ke</b> Internet Source	<b>&lt;1%</b>