FACULTY OF COMPUTING & INFORMATION MANAGEMENT

RESEARCH PROJECT

ON

DATA SECURITY: A TOOL TO ADDRESS CHALLENGES OF DATA CONFIDENTIALITY AGAINST DOMAIN USERS IN AN ORGANIZATION

By

DAVID KIBII CHERUIYOT
RegNo: 14/02098

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF SCIENCE IN DATA COMMUNICATION AND NETWORKING IN THE FACULTY OF COMPUTING AND INFORMATION MANAGEMENT AT KCA UNIVERSITY

NOVEMBER, 2016

DECLARATION

I **David Kibii Cheruiyot**, the undersigned, hereby declare that this research proposal is my original work and that it has not been presented to any other University, college or institution for higher learning other than KCA University.

…….. ……

David Kibii Cheruiyot Date

Student No: **RegNo: 14/02098**

This project has been presented for examination with my approval as the appointed supervisor.

Signed …… Date ……..

Dr. Alice Njuguna (Supervisor)

Faculty of Computing & Information Management KCA University

Signed …… Date ……..

Dr. Samwel Matende (Supervisor)

Faculty of Computing & Information Management KCA University

Signed ……..… Date ……...

Dean,

Faculty of Computing & Information Management KCA University

Acknowledgments

I would like to sincerely thank all those who made the delivery of this thesis possible. Your honest guidance, support and encouragement meant a lot to me.

I am grateful to all my supervisors Dr. Alice Njuguna and Mr. Samwel Matende for their fruitful support and guidance to this success. Their valuable contribution made it possible for me to achieve the objectives of this thesis. God bless you Dr. Alice and Mr. Matende.

I thank my dear Wife Viola Cheruiyot and my children Ian Kibet and Nicole Chelangat for their patience, encouragement and moral support throughout the time I was studying and as I was writing this thesis. May God continue to bless them abundantly.

Most of all I thank the almighty God for strength, resources and knowledge. May His name be praised.

ABSTRACTS

Threats resulting from authorized users, specifically insiders, pose as one of the most challenging security issues that many rganizaiooons face today. Insiders often attack using authorized access and with actions very similar to non-malicious behavior. Insider threat poses a great risk to organizations due to the mere fact that they have privileges and authentic access to confidential data. Safeguarding information protect organization's confidential data and other sensitive information that might compromise its operations and competitiveness. Insider attacks comprise of deliberate and unintentional access to an organization's system, network,

or data and intentionally exceeded or misused that access in a manner that negatively affects the confidentiality of the organization's information or information systems. Insiders attacks take many forms including worms, viruses, Trojan horse, detection or alteration of data, sabotage, espionage, fraud, theft of necessary data or destroy of data, financial loss or reputation damage. The insider threats usually compromise the Confidentiality, Integrity and Availability of data in an organization. However, this research emphasizes specifically on data confidentiality because confidential information may be misused to commit illegal activities in case it fall into the wrong hands. In addition, the disclosure of sensitive information can lead to loss of confidence and loyalty. Information is extremely valuable and central to performance of the organization therefore, breaching confidentiality may result in loss of productivity and destroy the business. The study proposes development of a security a tool that addresses data confidentiality by monitoring domain users' activities. The tool will monitor activities such copying, modification or deleting confidential data.

KEYWORDS

Insider, Insider threat, domain, domain users, data security, data confidentiality

TABLE OF CONTENTS

Contents

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

1.0 INTRODUCTION

1.1 Background of problem

Threats resulting from authorized users, specifically insiders, poses as one of the most challenging security issues that many rganizaiooons face today. Insiders often attack using

authorized access and with actions very similar to non-malicious behavior. Insider threat poses a great risk to organizations due to the mere fact that they have privileges and authentic access to confidential data. Furthermore, insider attack comprise of unintentionally enabled by users who tend to fall victim to external attacks.

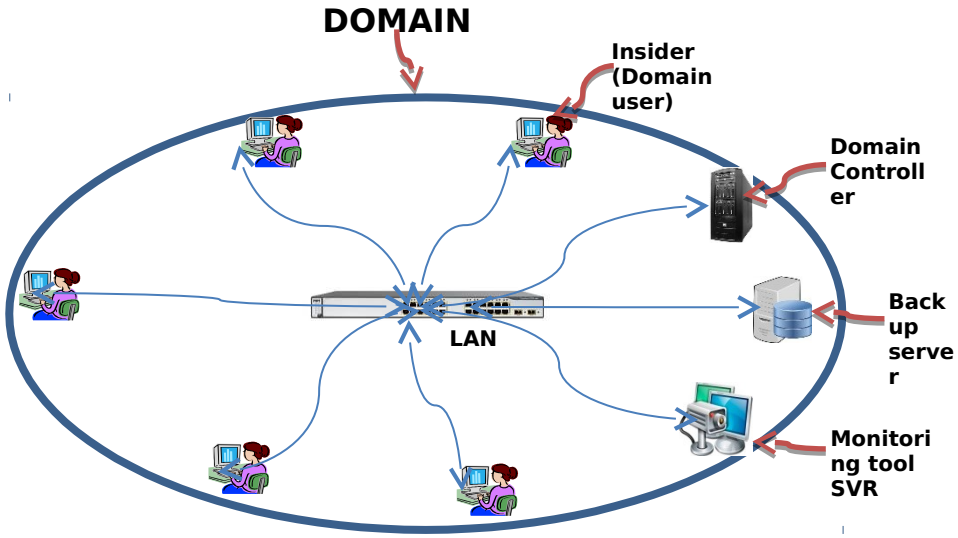
The insider threats usually compromise the Confidentiality, Integrity and Availability of data in an organization (National Cyber Security and Communications Integration Center, 2014). Insider threats are perpetrated by rogue administrators and users of the information systems who intentionally compromise data confidentiality, availability and the integrity.

The Computer Expert Response Team (CERT) Insider Threat Center defines a malicious insider as a "current or former employee, contractor, or other business partner who has or had authorized access to an organization's system, network, or data and intentionally exceeded or misused that access in a manner that negatively affect the confidentiality of the organization's information or information systems." (Flynn, Huth, Trzeciak, & Buttles, 2013) Since 2001, studies document over 700 cases that emanate from actual insider crimes. The crimes collected range across multiple sectors, include small companies to multi-national corporations, and cover several hundred types of exploits used by malicious insiders to harm an organization.

CERT considers the following excerpt as a situation involving insider threat, "*The insider was employed as a system administrator at a data-mining firm contracted by a victim organization to process customer information. Though unnecessary for the job function, the insider had access to servers and data owned by the victim organization. An unprotected file containing encrypted password information was found on one of these servers. The insider brute-force attacked over 300 passwords, accessed data belonging to dozens of the victim organization's customers, and downloaded millions of personal records. Fortunately, the information was never sold or released by the insider before arrest"* (CERT, 2016)

The research will review emerging approaches and explore experimental possibilities for

measuring the effectiveness of proposed solutions. It will focus on various types of insider threats related to data confidentiality and come up with a tool that will detect login activities and monitor what information users' access from the system.
The figure below represents the structure of a domain and how the proposed solution will be implemented.
Figure 1.1: **The Structure of a domain**



1.2 Causes of problem in research area

- **Organizational management**- Too much trust bestowed on system administrators by the management of the organization
- **The problem is not well understood**: Researchers need to also understand underlying human motivations and behaviors that encompass insider therat. Since this is not a outdated area of study for IT security academics; constructing technical answers to monitor for human dishonesty is challenging.
- **Data on insider attacks is difficult to obtain –** this is because there is a dilemma on how an insider who is supposed to provide his malicious deeds will expose himself
- **Ground truth data**: Organizations that experience insider attacks are often hesitant to share data about the attacks they are facing publicly. Studies evidence that over 70% of attacks are fail to meet external reporting, while many of the most common, experience low-level attacks. This leads to uncertainty that available data accurately represents the

true nature of the problem. In banking sectors where such exposures might be perceived negatively by customers is where the problem lies greatly.

- **Baseline data**: there are no studies that provide baseline data for insider attacks. As such, the rates are unknown; also, the actions of non-malicious users are also not presented in large data sets.

1.3 Definition of terms

- **Data Security**- Dorothy Denning, 1982: Data Security is the science and study of methods of protecting data from unauthorized disclosure and modification.
- **Data Confidentiality**- refers to whether the material kept on a system is protected against inadvertent or illicit access. Since systems are occasionally used to manage subtle information, Data Confidentiality is repeatedly a measure of the aptitude of the system to defend its data.
- **Insider Threats-** refers to a malicious **threat** towards an organization that stems from people inside the organization, such as employees, contractors, former employees, or business associates, who tend to possess inside information regarding the organization's security practices, computer systems, and data.
- **Domain** – Is a subnetwork made up of a group of clients and servers under the control of one central security database
- **Domain Users** – These are the insiders. Domain users refers to one whose username and password are kept on a domain controller instead of user is loggin into the system.

1.4 Problem statement

Ideally, Organizations needs to protect their confidential data against insider threats. This can be achieved by monitoring behavior and activities of login users in a domain such as copying modifying or deleting of crucial and confidential data.
Cybersecurity experts face noteworthy challenges in preventing, perceiving, and responding to insider attacks. They often turn to insider threats researchers for solutions. Regrettably, insider

threat scientists face grim barriers to conducting systematically and operationally usable work, such as access to real-world data and ground-truth about malicious insider activity. Technical tactics to this challenge are emerging, but studies show little noteworthy progress has been made in plummeting the actual numbers or influences of insider attacks.

This research will develop an information technology tool that will address the challenges specific to domain users who are the insider threat problem

1.5 Justification of the study

This research emphasizes specifically on data confidentiality because confidential information may be misused to commit illegal activities in case it fall into the wrong hands. Also, the disclosure of sensitive information can lead to loss of confidence and loyalty. Information is extremely valuable and central to the performance of the organization therefore, breaching confidentiality may result in loss of productivity and destroy the business. As such, it becomes important to protect confidentiality over integrity and availability.

1.6 Aims and objectives of the project

1.6.1 Aims (General Objective)

- To address challenges of data confidentiality against domain users in an organization

1.6.2 Specific Objectives (Identify, define, Design, Implement, test and validate)

- To identify how user behavior compromises the confidentiality of data in an organization.
- To develop an information technology tool that protects the confidentiality of data against users in a domain.
- To verify and validate the information technology tool to monitor the activities of users in a domain.

- To make policy commendations on the extenuation of threats posed by insiders on data confidentiality in an organization.

1.7 Research questions

- How does user behavior compromises the confidentiality of data in an organization?
- How emerging technologies does affect data confidentiality within an organization?

1.8 Significance of the study

The findings and the results of this study will be of great significance to the management of the organizations**.** The management will highly benefit from the study. This is because they will be able to understand the importance data confidentiality against the insider threats so that they improve on their data security policy.
Other researchers will use the findings of this research as a basis of their research on similar or related topics in the future. Furthermore, the research will review emerging approaches and explore experimental possibilities for measuring the efficacy of proposed solutions.

CHAPTER 2

2.0 LITERATURE REVIEW

2.1 Understanding the insider threat

An insider threat according to CERT refers to a current or former employee, contractor, or other business partner who has or had approved access to an organization's network, system, or data and intentionally misused that access to negatively affect the integrity, confidentiality, or availability of the organization's information or information systems (Wang, Han, & Liu, 2010).

Insider threats range from sabotage, theft, fraud, espionage, and competitive advantage are often carried out through abusing access rights, theft of materials, and mishandling physical devices (Ophoff at al., 2014

2.2 The insider

To achieve business objectives enterprise need to trust their employees to hold their business process workflow. But, trusting on employees working in organization does not guarantee the protection of confidential assets and sensitive data that stored in organizational databases. A very common and well outlined definition of an insider as an individual with privileged access to organization system (Roy, 2010). It is confounded by the recent developments in ubiquitous network computing and a blurred boundary definition of insiders and outsiders. Insiders have privileged access to the organizational information, system and networks. Insiders are most often recognized as employees, but also other people who relate to organization like contractors, business partners, auditors, suppliers, students, associates, etc. are concerned (Yang & Wang, 2011). Furthermore, the definitions of insiders differ for every organization according to their business policies and authorities. Nevertheless, we clarify a certain individual as insider if he or she fulfils one of the below listed requirements.

- A person who has privileged access to a computer system or network like workers, employees or staff members.
- An individual, who does not work in a company but has an organizational relationship with this company like contractors, business partners, auditors and suppliers etc.
- Someone, who has valid account to access the system from in or outside the company like student, alumni, former employees or currently discharged employee.
- Any officers or security staff having access to exclusive confidential and sensitive information.
- Anyone, who may not have logical privileged but physical access to the system, to the systems connection or simply to the data storage like sweeper, cleaning staff, delivery boy etc.

2.3 Characteristics of Insider

Every definition of Insider has some common characteristics which describe them in clear and detailed view. The mentioned characteristics are listed hereafter and will be used in this master's thesis to differentiate internal with external entities.

- **Trust:** When a Person is hired in a company, he or she is considered as a member of trusted group of organization. Trust has different meanings in case of security and social science. It means assurance and dependability. As compared to outsiders, trust is a fundamental characteristic of insiders (Yang and Wang, 2011). For what reason, insiders are trusted by default because they are considered as a part of the organization and therefore, they have trustworthy agreement with that organization.
- **Access:** Insiders have privileged access to the system. The process of accessing is distinguished in two ways as legitimate access and authorized access (Ophoff, 2014). Though, insiders have authority to access to the information but it may not need to know this information in detail to access it
- **Knowledge:** Insiders may have good knowledge about information, information system and services and also enhanced abilities to misuse it (Ophoff, 2014). E.g., a

person who develops software has no direct access to the system but has a good knowledge about software or system.

Along with the above stated characteristics of insiders, the organization control, for example a contract between employee and organization, can be considered as a legal authority by insiders who are different from outsiders

A research by Bishop on defining insider threat argued that majority of papers considers a binary approach to an insider. They have proposed a definition which can be extended in many domains.

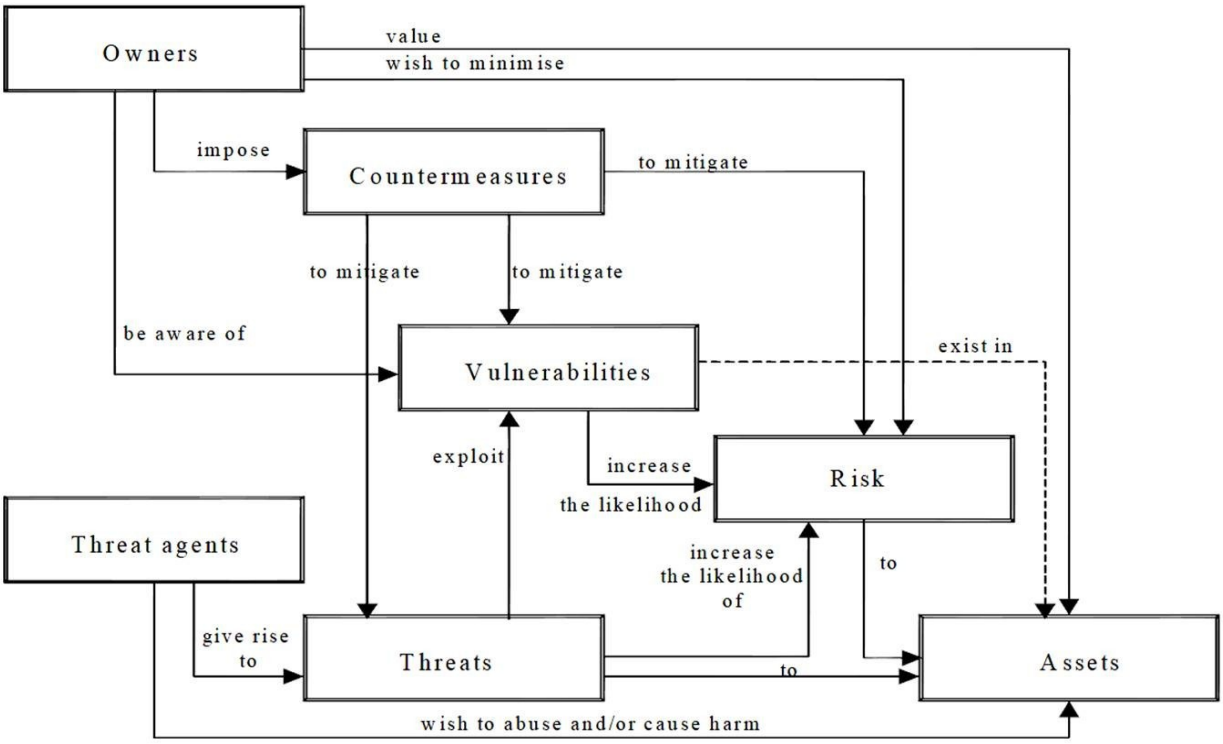


Figure 2.1: **Security Conceptual Framework (**Farahmand et al**)**

Insider is a trusted entity with the power to break one or more rules in a given security policy and the insider threat occurs when a trusted entity abuses that power (Samuel, 2010). It presents that insiders are determined with some set of rules which is a part of security policies. It is also believed that misuse of the rights and authorities given in organization causes insider threat. Misuse may come with meaning of violation of such rules which are partially written in legal, social, ethical aspects, rules those are un-observable and non-existent (Roy, 2010). An insider threat with very simple way has been defined in accordance of misuse. It is a term posed by an individual who misuses his privileges or where access to information results into

misuse.

When studying attacks by the insiders, it is quite helpful to look at methods and steps attended by insiders (Wang, Han, & Liu, 2010). Insider attack is not centered only on technical exposures. Fist attacker tries to identify which system has target data and who has access to it. Then, she steals credentials or conducts activities to cause harm to system and investigates such vulnerable points where more damage can occur with less effort. R. Stiennon has described an anatomy model of insider attack can be considered as good example.

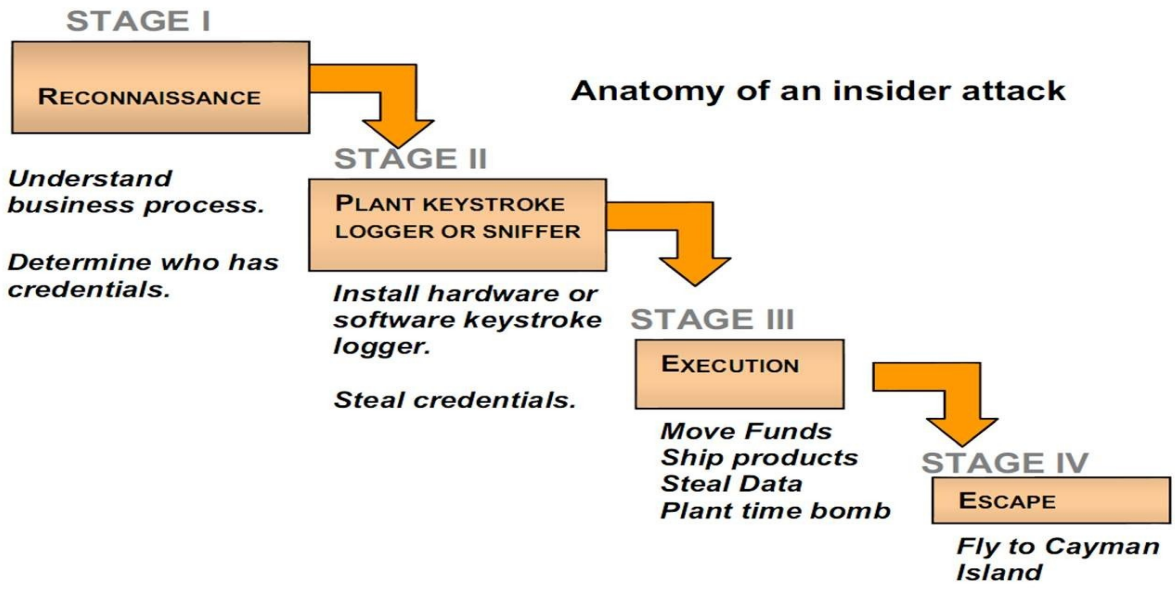


Figure 2.2 Anatomy of insider attack (R. Stiennon)

Attacks carried out by insiders takes many forms including worms, viruses, Trojan horse, detection or alteration of data, theft of necessary data or destroy of data, financial loss or reputation damage etc. J. Butts has developed an insider threat model using functional decomposition and categorized attack forms in four categories. We agree that every type of threat fits in one of these categories.

- **Alteration:** Includes modifying or deleting the information system in unauthorized manner.
- **Distribution:** Transfer of important data to other unauthorized entity.
- **Snooping:** Same like distribution but in snooping insider obtains unauthorized information on a user and distributes it.
- **Elevation:** When user get unauthorized rights to access system.

Insiders are always been a part of organization so there will be always a chance of getting affected by insiders. Insiders have endless opportunities to access private and valuable data and

other side to steal or harm company for their respective purposes. Not every insider is malicious. Some threats happen intentionally and some unintentionally.

2.4 Factors affecting Insider Threats

Many companies can often detect or control attacks on their data resources and can provide mitigation measures to threats by outsiders who tries to get access to information in unauthorized way. However, it is harder to detect an individual with legitimate access to organizational assets. A malicious insider has more potential to cause serious damage to sensitive data than outsider. Insiders have pre-knowledge about how, where and when to attack the system as they are a member of the organization. There exist many forms of technologies that present to protect information from malicious attack. Attacks are appropriate to detect and defend against but technical tools used to protect against these attackers are rather scalable and cost effective to apply on each individual who has given access to the system. As time passes, technology has been progressed with significant changes in social and cultural issues. Colwill (2009) believed that though technical measures are available to detect threats they cannot be considered isolated. Security measures are improving but technology alone is not enough to protect, some other organizational, personal and behavioral factors also considered altogether with technical factors. There are varieties of purposes and factors which may increase likelihood to detect threats to confidential data of organization. To deal with insider threats in detection or protection, it is very important to know about what factors affect them.

2.5 Challenges with the insider threat

Eliminating insider threats requires efforts be directed towards preventing the insider from attacking. There exist a number of challenges to addressing and reducing insider threats facing computer systems in organizations.

2.5.1 Rapid technological developments

Ever growing technologies result in diminished boundaries, while security against insider threats persists as boundary driven. This new technology enables malicious attackers to initiate attacks that do not have immediate consequences, thus making them feel less culpable. The technology also allows insiders to launch virtual actions that expose stored data while at the same time retaining their anonymity. In addition, the problem of outsourcing persists.

2.5.2 Lack of data

The literature on insider threats is not vast enough to facilitate development of technologies and mechanism to protect organization from insider threats. The available literature is scanty, subjective, and unreliable. Furthermore, organizations and corporations are unwilling to share cases of violation by insider for the fear of reputation as well as that of competitive disadvantage. Because of inadequacies in available literature, solving the problem of insider threat remains challenging.

2.5.3 Minimal education and awareness

There lacks common understanding of insider threats among security professionals. As such, security professionals are unable to convince organizations to invest in technologies and mechanisms that mitigate insider threats. More so, education and awareness among security practitioners seems to be differing, yet it is the critical component of addressing insider threats. According to Noonan and Archuleta, (2008) education and awareness are key to successful insider threat elimination.

2.6 Mitigation Strategies

Recommended strategies to combat insider threats include a multi-dimensional approach implemented at various layers of security. The most recommend approaches include:

2.6.1 Technical approaches

Combating insider threats from a technological perspective requires use of technology for detecting suspicious insiders and preventing them from accessing data (Bowen, Salem, Hershkop, Keromytis, and Stolfo, 2009). Nonetheless, the approaches should have an integration of monitoring and auditing techniques that allow monitoring of systems such that it becomes easy to identify person responsible for the insider threat.

The problem with monitoring and auditing approaches is that they do not solve the problem, that is, they do not mitigate insider threats. Instead, the approaches applied at monitoring and auditing levels helps capture evidence for insider threat but does not prevent insider threat from occurring. Enforcing technological security against insider threat requires integration with policies defining permissible behavior within organization. The policies stipulate set of expected behavior that provide a foundation for access and data use (Hunker and Probst, 2008). However, use of policies has given rise to complexity of human behavior, thus should be integrated with physical access restriction. Hunker and Probst, (2008) recommend monitoring technologies as a means to mitigate insider threats. Monitoring involves installing devices to capture human activity on computers. Such monitoring can take format of misuse detection to identify misuses based on anomaly and rule base detection that differentiates normal behavior from standard deviations. Monitoring activities can take place at network or host level. Unfortunately, installing host sensors is difficult unlike network sensors. That problem is insider threats are unlikely to happen at the network layer.

Another significant problem with technological monitoring is that it lacks human aspects of insider behavior. A monitoring technology is unlikely to capture elements such as reason behind anomaly behaviors such as working overtime is for good or malicious purposes (Crampton & Huth, 2010).

2.7 Existing tools

Table 2.1 Comparison with the existing solutions

No	Attributes	Windows Active Directory	Cyberoam Appliance (UTM)	Linux	Kaspersky security center	Ethical Hacking Tools	Proposed Babysitter tool
1	USB storage device locker (Bitlocker) policy	✓	X	X	✓	✓	✓
2	USB port monitoring	X	X	X	✓	✓	✓
3	Domain users Monitoring	✓	X		✓	✓	✓
4	Ability to identify the source of insider attacks	x	x	x	✓	✓	✓
6	Need for investigation	✓	✓		✓	✓	x
7	Ability to capture remote logins attempt	✓	x		x	x	✓
8	Stealth monitoring technology	x	x	x	x	✓	✓
9	Need for expertise	✓	✓		✓	✓	x
10	Need for third party software	✓	✓		x	x	x
11	Ability by non-admin users such auditors and managers to use	x	x	x	x	x	✓
12	Inclination to Outsider threat	x	✓	x	✓	✓	x

CHAPTER 3

3.0 RESEARCH METHODOLOGY

This section provides a brief overview of popularly used solutions

3.1 Detect and deter

It is worth noting that one recent study names local area network (LAN) access as the top vector for insider threats/misuse (71%), followed by physical (28%) then remote access (21%). The following offers detection, prevention and deterrence methods to consider.

4.6.1 Data encryption

Drive-level encryption is built-in, although optional, in Windows and Mac OS X. Requiring the use of encrypted portable drives will thwart data loss in case of loss or theft. At an OS-level, a variety of vendors market data loss prevention (DLP) products which can encrypt files on the fly -- that is to say, when they are copied to other devices. These encrypted files will require company-provided keys to unlock. Data encryption is a strong defense against careless data loss, but it is not particularly useful again deliberate data theft. Insiders who have access to sensitive data will necessarily have the credentials to decrypt it. Against this type of threat, the best technical defenses must address the ability for data to be removed from the organization.

3.1.2 Data access monitoring

Data access monitoring helps the system admin to observe who accessed data, at what time, and on what computer. This means of protection against insider threats makes it possible to identify who has access to what data. When data is accessed, the system admin will be able to know what data has been accessed and by who. This makes it possible to pinpoint who the insider is and can be identified to face disciplinary action.

3.2 SIEM and log analysis: Security information and event management

3.2.1 Data loss prevention

Data reduction: This refers to minimizing the amount of information accessible to insiders. It means constantly offloading data from users' computers as well as online storage system

accessible to users thereby minimizing the amount of data. This way, there will be little or no information to steal from the organization. This is not an effective means of protecting against insider threats because it does not prevent users from accessing or retrieving the data. It only minimizes the available data.

3.3 Enterprise identity and access management

Data access control: This is a means to controlling who has access to data. It gives users authority using security level clearance system. According to level of clearance, the user access data privileged under their clearance. Still, this method prompts accessibility of data because insiders have clearance to access certain amount of information.

3.4 Enterprise digital rights management solution

3.4.1 Deterrence methods

Deterrence methods include:
Deploy data-centric, not system centric security
• *Crowd-source security*
• *Use positive social engineering*
• *Think like a marketer and less like and IDS analyst*
• *Build a baseline based on volume, velocity, frequency and amount based on hourly, weekly, and monthly normal patterns*
• *Use centralized logging to detect data exfiltration near insider termination28*
• *Require identification for all assets (e.g. access cards, passwords, inventory check out)*
• *Note frequent visits to sites that may indicate low productivity, job discontent and potential legal liabilities*

3.5 Authorization and authentication

The computer security world defines *access control* as providing or limiting access to electronic resources (we can also say granting or limiting trust) based on some set of credentials. Access control typically consists of two components: *authentication* and *authorization*. Authentication is showing who (or what) you are; i.e., demonstrating possession

of certain credentials. Authorization is the system determining if your credentials are sufficient to provide you with a requested type of access.

3.6 Securing Data Portability

Preventing data leakage is a difficult task for any company considering the various ways data can be transferred to other media or over the Internet. While it will be near impossible to block every vector without interfering with routine business there are some mechanisms a company can employ to reduce this threat.
Fortunately there are tools and applications that companies can use to restrict this access such as DeviceLock, Sanctuary Device Control, and USB Blocker. These are applications managed at the enterprise level that can be used to monitor and prevent the installation or use of USB media or CD/DVD drives on workstations. This can prevent employees from exporting mass amounts of intellectual property onto a thumb drive and taking it home. There are also ways of manipulating Windows Group Policy Objects (GPO) to restrict USB access, but this has been difficult to achieve in practice. If an employee is suspected of removing intellectual property on a thumb drive, this can be validated in the registry by examining the registry using "regedit.exe" and looking up the following key.

3.7 Definition of the tool to adopt

After comparison of various methods employed against insider threats, it is apparent that the problem persists. Therefore, a holistic approach to protecting data against insider threats is important. Methodology of this study proposes implementation of a tool on server on a domain that will facilitate monitoring data access and at the same time report malicious activities. The tool is server-side supported and monitors users in a domain without notification. The tool will monitor login activities on end user

computers, data access, and who delete, modify or copies what data to the external drives.

System logs will build up very rapidly so it will be important to establish filters or alerts to notify security teams in the event of a critical change or incident. Due to the overwhelming amount of data that can be logged, these filters should be tuned to ignore standard business operations but highlight anomalous activity.

3.8 Method/proposed method

The architecture including a monitor platform (MP) has been proposed in order to make the internal users on the host, network effectively, prevent violations from internal, and enhance their internal security. Organizations must monitor all critical information system activity like servers, software applications and other data resources, Access must be strictly controlled and any suspicious activity must be investigated. MP has a powerful logging system. As shown in literature, an improved surveillance method based on complex roles has been proposed in order to monitor the work activities of the users in organizations, applications and operating systems.

Currently, MP launched by software companies is generally composed of three parts: Client, server-side and management-side. Client is the agent installed on the computer software. It is used to collect host data and receive the security policies and directives configured by the administrator from the server-side. Its ultimate aim is to monitor the host behavior. Server-side is installed in a platform with the high performance. It is used to receive various kinds of information sent by the host client. And then the information can be managed and stored. Management-side is usually a web service or other applications. After users logging in, managers can access the corresponding management interface. Appropriate security policy is configured and issued. Client log can be inquired and analyzed. A variety of statistical information can be counted and managed. The following functional areas should be included in

a comprehensive network of Monitoring Platform: firstly, desktop management and control of host behavioral. Secondly, internet behavior management and breaking of illegal host access; thirdly, security management of terminal equipment and storage media; fourthly, remote installation of system patches distribution and software; what is more, monitoring and safety assessment of the host system performance; in the end, monitoring of network equipment.

3.9 Study design

The study sought to identify how user behavior compromises confidentiality of data in an organization. To help address this objective the study interviewed IT experts from three organizations. The searcher randomly sampled three organizations from a list of twenty-one organizations. Random sampling in this instance was preferable because it provided organizations with an equal chance to be selected.

3.9.1 Setting and sample

The study was interested with security professionals of these organizations. Therefore, the researcher developed introductory letters addressing them to the organizations requesting them for their cooperation. In the letter, the researcher mentioned the purpose of the study. The researcher sampled three organizations namely KCB, Safaricom, and Nation Media Group. In each of the three organizations, the researcher sampled three security professionals. Therefore the study comprised of a sample of N=9

3.9.2 Confidentiality

The researcher intended to uphold the confidentiality of participants by holding them anonymous to research report. The study would not collect any identifiable information that would expose the identity of participants. In addition, the researcher sent introductory letters to the participants requesting them for their consent in the study. The letter also informed participants to refrain from providing any personal identifiable information.

3.9.3 Measurement and instruments

The researcher used a structured interview for collecting information (refer to Appendix II). The research and ethics body of the University approved the interview transcript. The interview would assess user behavior that compromised data confidentiality.

3.9.4 Limitations

The researcher faced numerous limitations in data collection. Firstly, the researcher experienced shortage in amount of time need to conduct exhaustive data collection. This limited the number of persons that the interview would interview. Secondly, there was problem with allocating time of interview as the participants had busy schedules.

CHAPTER 4:

4.0 IMPLEMENTATION AND RESULT ANALYSIS

4.1 Introduction

To protect information assets and to keep the health of the network at an appropriate level, we have developed standardized log file monitor/filter. It consists of four modules. Figure 1 depicts the system architecture.

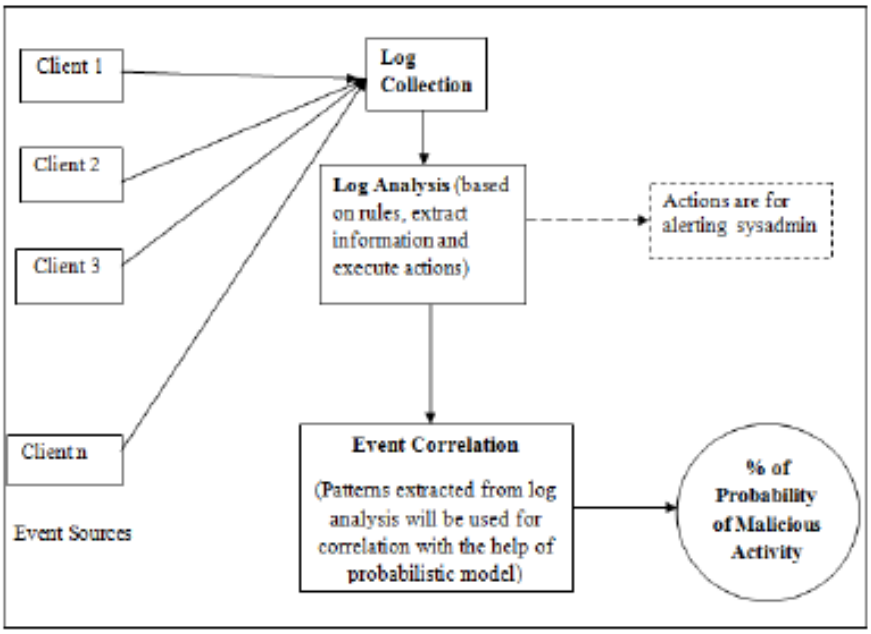


Figure 4.1 log file monitor architecture

Each module has a specific, well-defined task to perform. Each module passes on the data ahead. Four modules are mentioned below

- Module 1 : Log Collection
- Module 2 : Log Analysis
- Module 3 : Event Correlation
- Module 4 : Calculate probability

Module 1: Log collection

Log files are significant data source in this operation. Collecting data from many different

resources gives system administrators and security experts a picture of the current state of the network. In this proposed technique, it uses log file as the basic input into event correlation system. Log file is composed of individual log entries, which are, consists of a single line of text. These Log records are collected at server from different clients. The following section describes the actual log collection process.

The proposed tool monitors domain users' activities including that of network or system administrators. The tool will monitor activities such copying to a **USB storage devices**, modification or deleting confidential data

The proposed tool captures **logs** on the use of **USB** and other form of **storage devices** such as flash disk, pen drive, memory card, mobile phone storage, external flash drive, cd rom, IPad-wired

The capture format log

Log ID	**UserName (loginName)**	**Host Name**	**IP Address**	**mac address**	**External StorageType (USB)**	**FileName (Copied)**	**Path (Copied from)**
1	Cheruiyot	Com1	192.168.20.5	cm-ax1	Phone storage	Financial status	C:\Users\Admin\D-top\ F-status.doc

When computer users insert a USB on a computer within the domain, the tool will capture and display any traffic passing over USB connections. The captured communication data is stored in human-readable form, allowing the administrator to review exchanged data and perform effective forensic analysis on the transmitted data. The major advantage of the proposed toll is its ability to process monitored information in real time. The following is a capture format in real time monitoring:

Log ID	**UserName (login Name)**	**Host Name**	**IP Address**	**mac add**	**Time**	**External Storage Type(USB)**	**FileName (Copied)**	**Path (Copied from)**

1	Cheruiyot	Comp 1	192.168.20.5	cm-ax1	02:05PM 7/28/2015	Phone storage	Financial status	C:\Users\Admin\Desktop\Financial status.docx

The tool installs filter driver between USB host controller diver and device drive, and then monitors all USB Request Blocks, displaying them in easily readable format. Since all insider threats are not only executed using USB tools, the proposed tool monitors outgoing Bluetooth files and outgoing wireless connection files. The tool monitors activity of Bluetooth devices connected to the domain, and displays a log of Bluetooth devices. Every time a device is connected or leaves connection a new log line is added. The following information is recorded:

Log ID	**UserName (LoginName**	**Host Name**	**IP Address**	**Mac Address**	**Device name**	**Event time**	**Event type**	**File Name**
1	Cheruiyot	Com 1	192.168.20.5	cm-ax1	Techno	02:05PM, 7/28/2015	Copy	Financial status

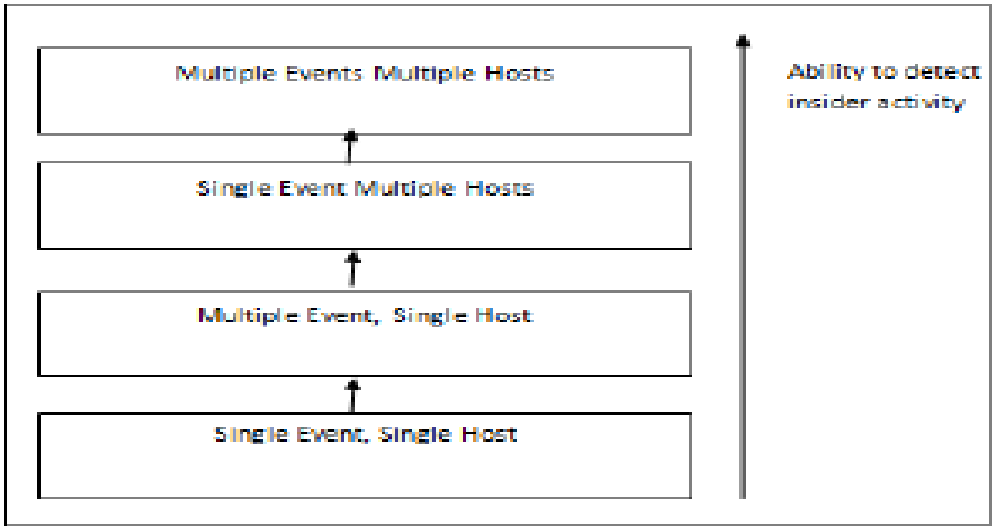
Module 2: Log analysis

To be able to handle input events irrespective of their format, regular expression is used for recognizing them. Rule based approach is used here for processing events and for eliminating unwanted data. This rule based approach has a specific format which consists of certain fields [1]. The *type* field indicates the type of rule. Next, the *pattern* field of the rule defines the pattern for recognizing input events, while the *ptype* field defines its type. The *desc* field of a rule defines the scope of event correlation and influences the number of operations created by the rule. The significance of *action* field is that when input message will match the regular expression pattern of any particular rule, it will fork a command

Module 3: Event correlation

Simply anything which happened at some moment in time which is defined as an event could be an action or occurrence identified by a program, such as pressing a key or clicking a mouse

button. In computing environment, the term event is also used for that message which conveys what has happened and when it has happened. Hence, to define event or a sequence of events on individual system or a group of systems is useful in the detection of insiders. As more clients are added, the ability to correlate activities which are happening across the network increases. Figure 3 shows that with each successive increasing level of the hierarchy, new type of behaviour may be detected and hence the ability to detect malicious activity also increases.



Module 4: Calculate Probability

Effectiveness is one of the characteristic of the intrusion detection. It defines to what degree it can detect the intrusions and how good it is at rejecting false alarms. In order to find intrusive behavior probabilistic approach is used in this work.

4.3 Findings

This part discusses the results of interview conducted in three organizations namely, KCB, Safaricom, and Nation Media Group. The objective was to gain insight into user behavior and identify how this compromises the confidentiality of data in an organization. Specifically, to identify how user behavior compromises the confidentiality of data. The study used interview approach to collect information from the organizations (Refer to appendix 1 for interview transcript). The interview assessed control behaviors as perceived by the security professionals

interviewed. In addition, the interview also assessed various mitigation strategies applied by the organizations.

4.3.1 Role of respondents

The study interviewed nine personnel from three different organizations namely Safaricom, KCB, and Nation Media Group. Each organization produced three respondents. All of the study respondents were in charge of information security management, that is, they had a technical role in information security of the organization. This ensured that information provided was derived from persons knowledgeable about insider threat.

4.3.2 The insider threat

The respondents reported being aware of insider threat; 100% of respondents had knowledge of what insider threat is, and acknowledged that their organizations face insider threats. They identified internal users as the biggest threat to security in the organization. Respondents also mentioned that compromise of information security by employees through disclosure, data leakage, and password compromise as frequent threats facing organization. Fraud and industrial espionage also emerged as internal behaviors that propagated threat to information. The following table provides summary of various insider threats organizations face:

Insider Threats
Use of officially granted access to system and information for personal use
Information security threat emanating from internal staff
Corrupt staff engaging in fraud
Data leakage, disclosure, and password compromise because of compromise to information by employees
Internal users of the systems are the largest threat to security

Table 4.3.1 summary of various insider threats

4.3.3 Types of insider threats

In order to establish what types of insider threats that organizations experience, respondents were asked to mention the types of threats their institution had experienced.

Table 4.3.2 ranks types of insider threats depending on frequency of encounter:

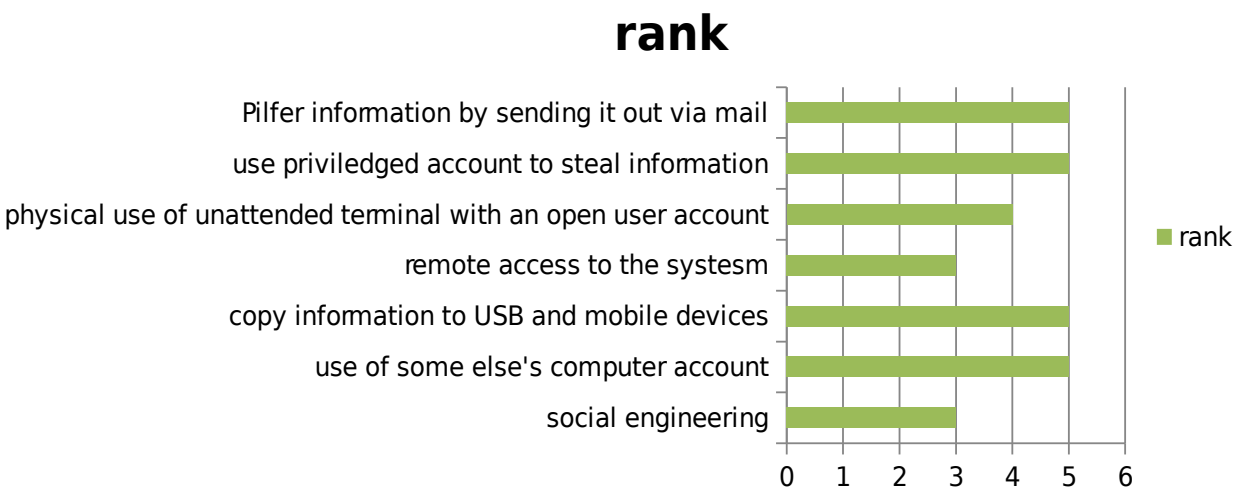
Types of insider threats	**Ranking**
unauthorized or illegal attempt to vie, retrieve, disclose, delete, or change information	1
unauthorized access to information systems	1
unintentional exposure to private information	2
illicit communication with unauthorized recipients	3
illegal generation of spam email	3
tampering with information system	4
denial of service attack	4
intentional exposure of customer records	5

According to the CERT 2011 Cyber Security watch survey (CERT, 2011), unauthorized access to / use of corporate information was the most prevalent insider threat, followed by unintentional exposure of private or sensitive data.

4.3.4 Mechanisms used to propagate insider threats

Respondents were required to identify mechanisms that were used by insiders to perpetrate insider threats.

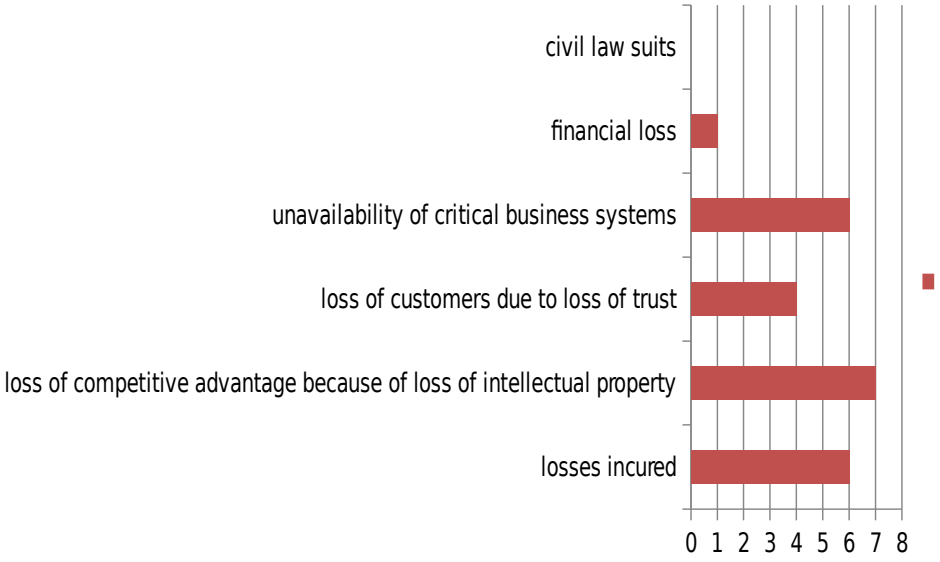
Figure 4.1 ranks the mechanisms starting with the mechanism used commonly.



4.3.5 Loss incurred

The type of loss experienced due to insider threats was evaluated in this section. Financial loss was the most likely result of an insider threat according to the research findings. Figure 4.2 summarizes the loss encountered by victim institutions. It should, however, be noted that the statistics on figure 4.2 do not indicate the sums of money lost but instead shows an admission of loss

Figure 4.2 summarizes the loss encountered by victim institutions



4.3.6 Criticalness of insider threat

Respondents were asked if their respective organizations consider insider threat to be a critical threat to information assets. All the respondents agreed that their organizations were taking insider threats seriously. Owing to losses suffered and sensitivity of personal information stored in their databases, respondents said that their organizations consider insider threat with great intensity.

When asked if their organizations have a formal insider threat handling process, the respondents agreed that the organizations have formal insider threat handling process

4.3.7 Mitigation strategies

The aim of this section was to identify formal, informal and technical mitigation strategies that financial institutions use to mitigate the insider threat.

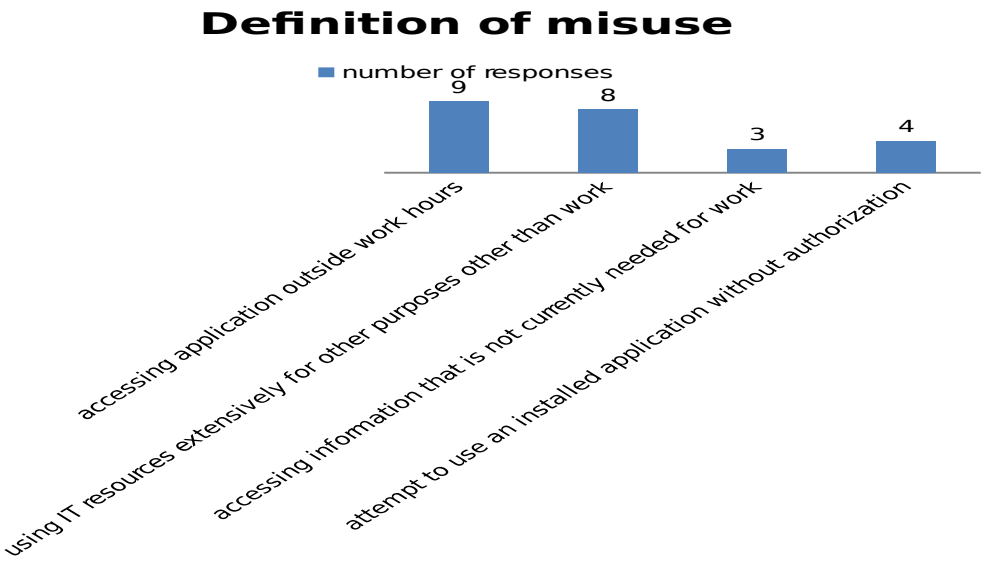
Mitigation strategies in use

Respondents were asked to select the measures that they had in place to combat insider threat. Institutions utilized a combination of technical, social and social-technical approaches. However, technical approaches were the most commonly used mitigation approaches.

Mitigation strategies
intrusion detection
monitoring and logging
risk management
encryption
role based access control
security education
physical access control
security policy
remote access and authentication
application controls
Pre-employment screening

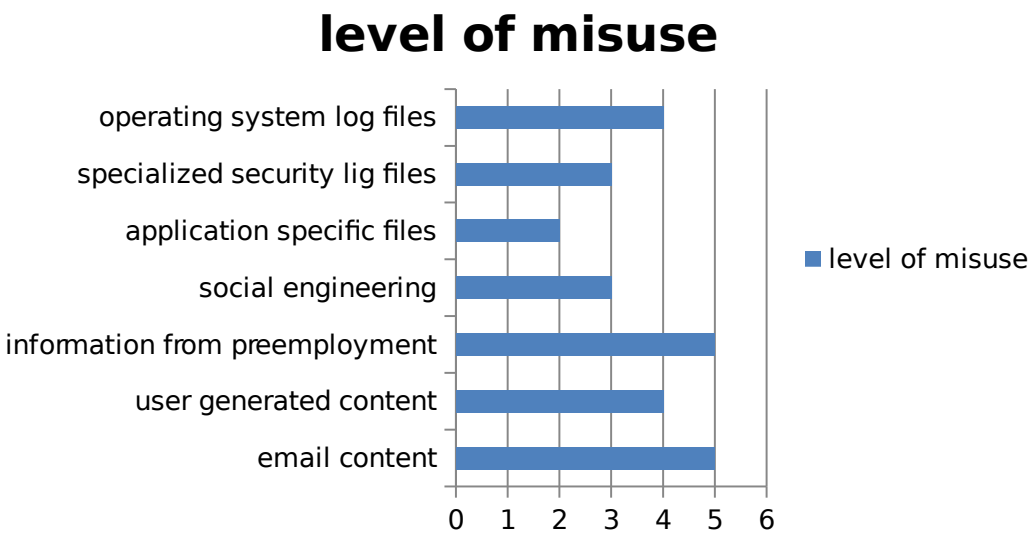
Misuse as defined by security policy

To gain insight into how institutions define insider misuse, respondents were asked to what extend does their security policy defines as insider misuse. The results showed that mostly attempting to install applications without authority and use of IT resources excessively for purposes other than for work were least considered insider threat. The objective of this question was to investigate an important aspect of handling the insider threat that is discovering some generic characteristics of a legitimate user who breaches security. This question, therefore, looked to determine activities that could be considered misuse.



Identification of insider misuse

Respondents were asked to select the most indicative sources of signs of insider misuse. This question provides insight into how insider misuse can be traced easily. From the results of the survey, monitoring and auditing were the most commonly used forms of identification of insider misuse.



Effectiveness of mitigation strategies

This section aimed to evaluate the effectiveness of mitigation approaches identified. Technical approaches which include audit, logging, monitoring were found to be the most effective. These results can be attributed to the fact that these institutions mostly employ technical approaches the table below

4.4 Operation of the tool

The ‘insider threat detection’ tool works in stealth technology, monitoring the activities of computer users. It records input and output files as well as requests to copy files into external storage. The tool arranges these actions in tokens and sends over the server for storage and processing.

4.4.1 Screen Shots

a) **Table 4.1: Table design**

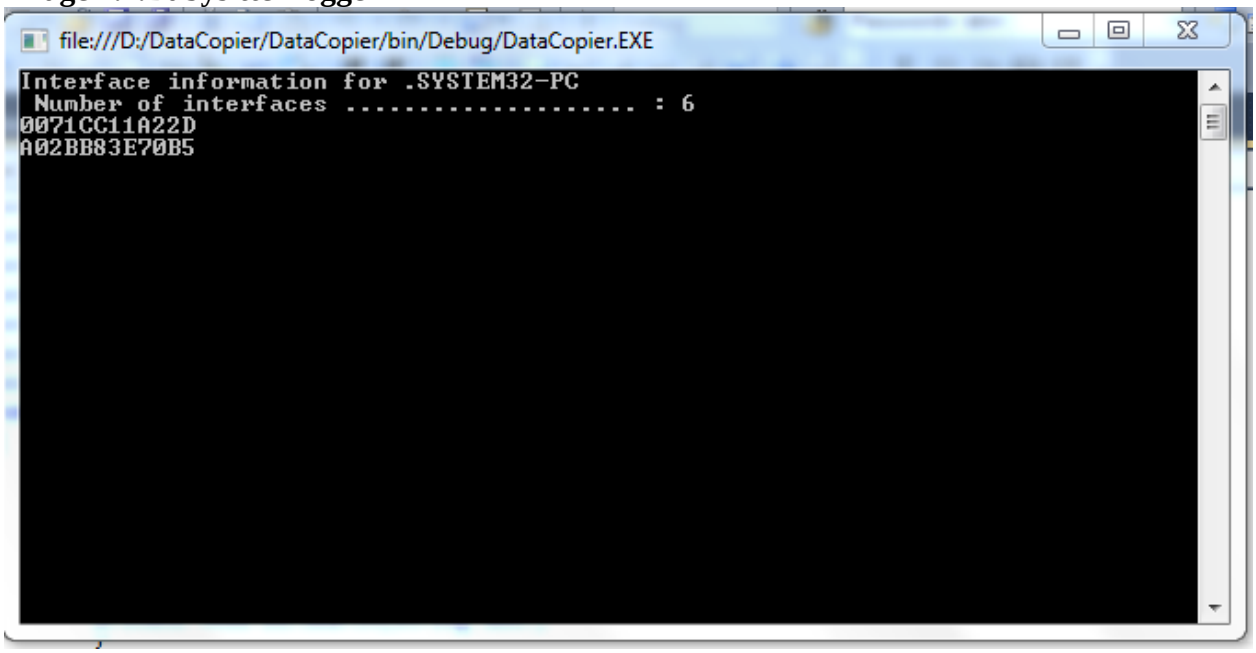
SYSTEM32-PC\SYST...bo.tblDataCopier | SQLQuery1.sql - S...ier (Amtech (57))*

Column Name	Data Type	Allow Nulls
CopierId	int	☐
LoginId	varchar(50)	☑
UserName	varchar(50)	☑
HostName	varchar(50)	☑
IPAddress	varchar(50)	☑
MacAddress	varchar(50)	☑
StorageType	varchar(50)	☑
FileName	varchar(250)	☑
Path	varchar(250)	☑
DateTime	datetime	☑
ModifiedOn	smalldatetime	☑
ModifiedBy	varchar(50)	☑
CreatedOn	smalldatetime	☑
CreatedBy	varchar(50)	☑
		☐

b) Baby sitter in stealth mode

This will be set to run on a stealth mode on client computers. User will not know when it is running but will be logging all the activities of that login user(s). When run on client computer, stealth mode hides it from being visible to the user.

Image 4.1.Babysitter logger



A screenshot of "insider threat detection" tool

On the server side, the admin must log into the system in order to generate logs. The following screen helps the admin to log in.

Image 4.2: Admin login to Database Server

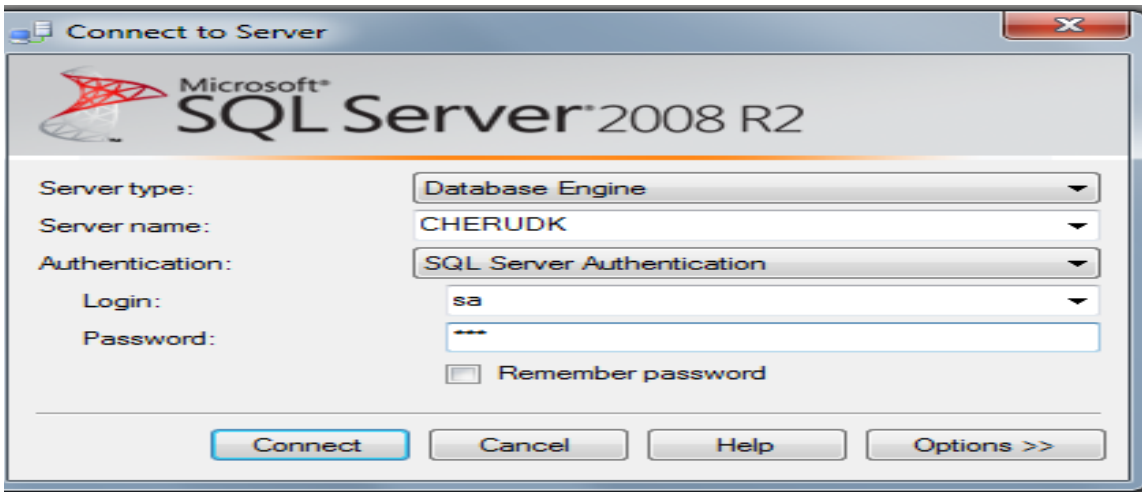
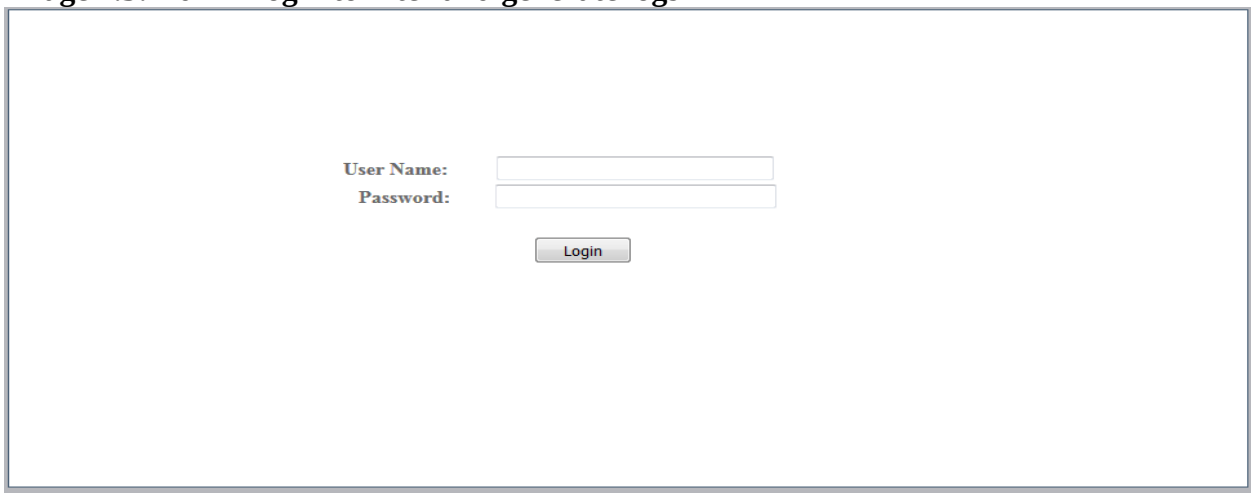
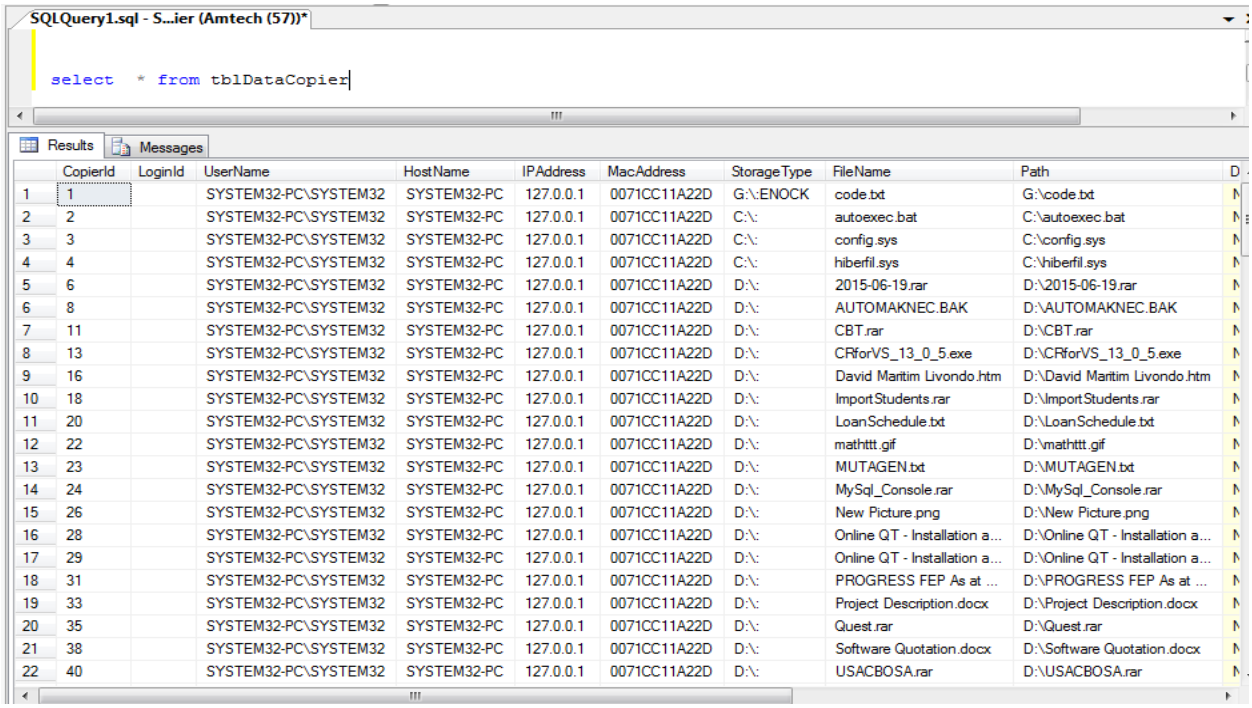


Image 4.3: Admin login to filter and generate logs



The admin logs on to the insider threat detection tool using a dynamic domain name, account name, and password. After logging on to the tool, the admin will see a user interface that consists of menu, tool bar, status bar, and main area. On the left side of the tool is the tree of computer and user group on the network. The tool's right side consists of main area where the admin views data. The tool appears as follows on the server computer

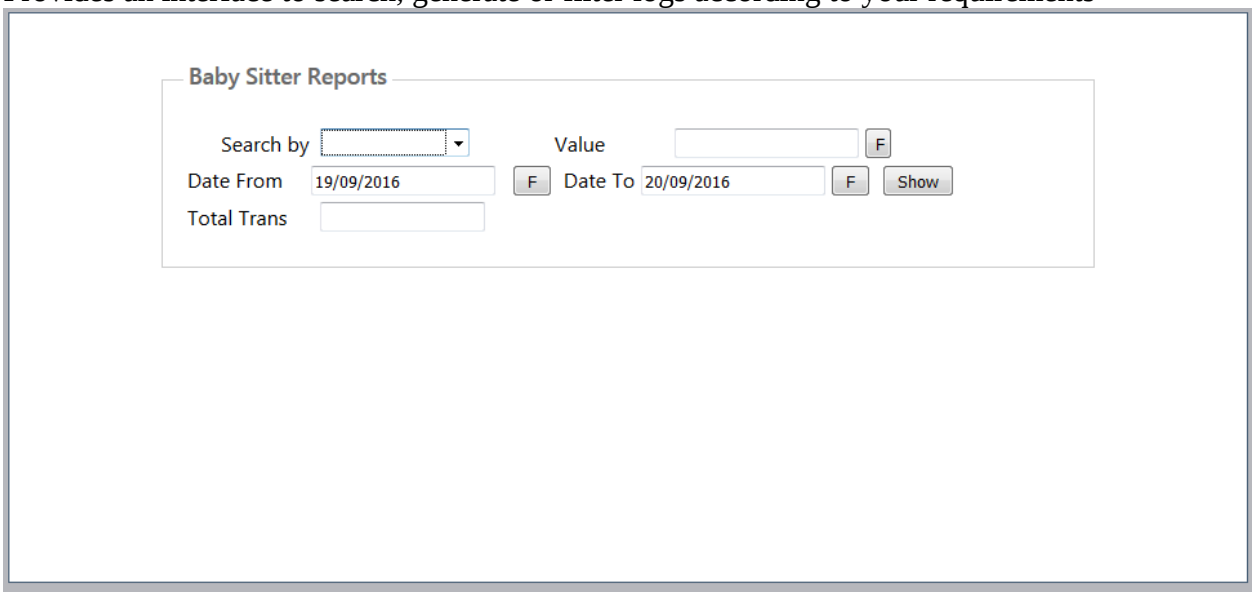
c) **Table 4.2: Table output**



	CopierId	LoginId	UserName	HostName	IPAddress	MacAddress	StorageType	FileName	Path	D
1	1		SYSTEM32-PC\SYSTEM32	SYSTEM32-PC	127.0.0.1	0071CC11A22D	G:\:ENOCK	code.txt	G:\code.txt	N
2	2		SYSTEM32-PC\SYSTEM32	SYSTEM32-PC	127.0.0.1	0071CC11A22D	C:\:	autoexec.bat	C:\autoexec.bat	N
3	3		SYSTEM32-PC\SYSTEM32	SYSTEM32-PC	127.0.0.1	0071CC11A22D	C:\:	config.sys	C:\config.sys	N
4	4		SYSTEM32-PC\SYSTEM32	SYSTEM32-PC	127.0.0.1	0071CC11A22D	C:\:	hiberfil.sys	C:\hiberfil.sys	N
5	6		SYSTEM32-PC\SYSTEM32	SYSTEM32-PC	127.0.0.1	0071CC11A22D	D:\:	2015-06-19.rar	D:\2015-06-19.rar	N
6	8		SYSTEM32-PC\SYSTEM32	SYSTEM32-PC	127.0.0.1	0071CC11A22D	D:\:	AUTOMAKNEC.BAK	D:\AUTOMAKNEC.BAK	N
7	11		SYSTEM32-PC\SYSTEM32	SYSTEM32-PC	127.0.0.1	0071CC11A22D	D:\:	CBT.rar	D:\CBT.rar	N
8	13		SYSTEM32-PC\SYSTEM32	SYSTEM32-PC	127.0.0.1	0071CC11A22D	D:\:	CRforVS_13_0_5.exe	D:\CRforVS_13_0_5.exe	N
9	16		SYSTEM32-PC\SYSTEM32	SYSTEM32-PC	127.0.0.1	0071CC11A22D	D:\:	David Maritim Livondo.htm	D:\David Maritim Livondo.htm	N
10	18		SYSTEM32-PC\SYSTEM32	SYSTEM32-PC	127.0.0.1	0071CC11A22D	D:\:	ImportStudents.rar	D:\ImportStudents.rar	N
11	20		SYSTEM32-PC\SYSTEM32	SYSTEM32-PC	127.0.0.1	0071CC11A22D	D:\:	LoanSchedule.txt	D:\LoanSchedule.txt	N
12	22		SYSTEM32-PC\SYSTEM32	SYSTEM32-PC	127.0.0.1	0071CC11A22D	D:\:	mathttt.gif	D:\mathttt.gif	N
13	23		SYSTEM32-PC\SYSTEM32	SYSTEM32-PC	127.0.0.1	0071CC11A22D	D:\:	MUTAGEN.txt	D:\MUTAGEN.txt	N
14	24		SYSTEM32-PC\SYSTEM32	SYSTEM32-PC	127.0.0.1	0071CC11A22D	D:\:	MySql_Console.rar	D:\MySql_Console.rar	N
15	26		SYSTEM32-PC\SYSTEM32	SYSTEM32-PC	127.0.0.1	0071CC11A22D	D:\:	New Picture.png	D:\New Picture.png	N
16	28		SYSTEM32-PC\SYSTEM32	SYSTEM32-PC	127.0.0.1	0071CC11A22D	D:\:	Online QT - Installation a...	D:\Online QT - Installation a...	N
17	29		SYSTEM32-PC\SYSTEM32	SYSTEM32-PC	127.0.0.1	0071CC11A22D	D:\:	Online QT - Installation a...	D:\Online QT - Installation a...	N
18	31		SYSTEM32-PC\SYSTEM32	SYSTEM32-PC	127.0.0.1	0071CC11A22D	D:\:	PROGRESS FEP As at ...	D:\PROGRESS FEP As at ...	N
19	33		SYSTEM32-PC\SYSTEM32	SYSTEM32-PC	127.0.0.1	0071CC11A22D	D:\:	Project Description.docx	D:\Project Description.docx	N
20	35		SYSTEM32-PC\SYSTEM32	SYSTEM32-PC	127.0.0.1	0071CC11A22D	D:\:	Quest.rar	D:\Quest.rar	N
21	38		SYSTEM32-PC\SYSTEM32	SYSTEM32-PC	127.0.0.1	0071CC11A22D	D:\:	Software Quotation.docx	D:\Software Quotation.docx	N
22	40		SYSTEM32-PC\SYSTEM32	SYSTEM32-PC	127.0.0.1	0071CC11A22D	D:\:	USACBOSA.rar	D:\USACBOSA.rar	N

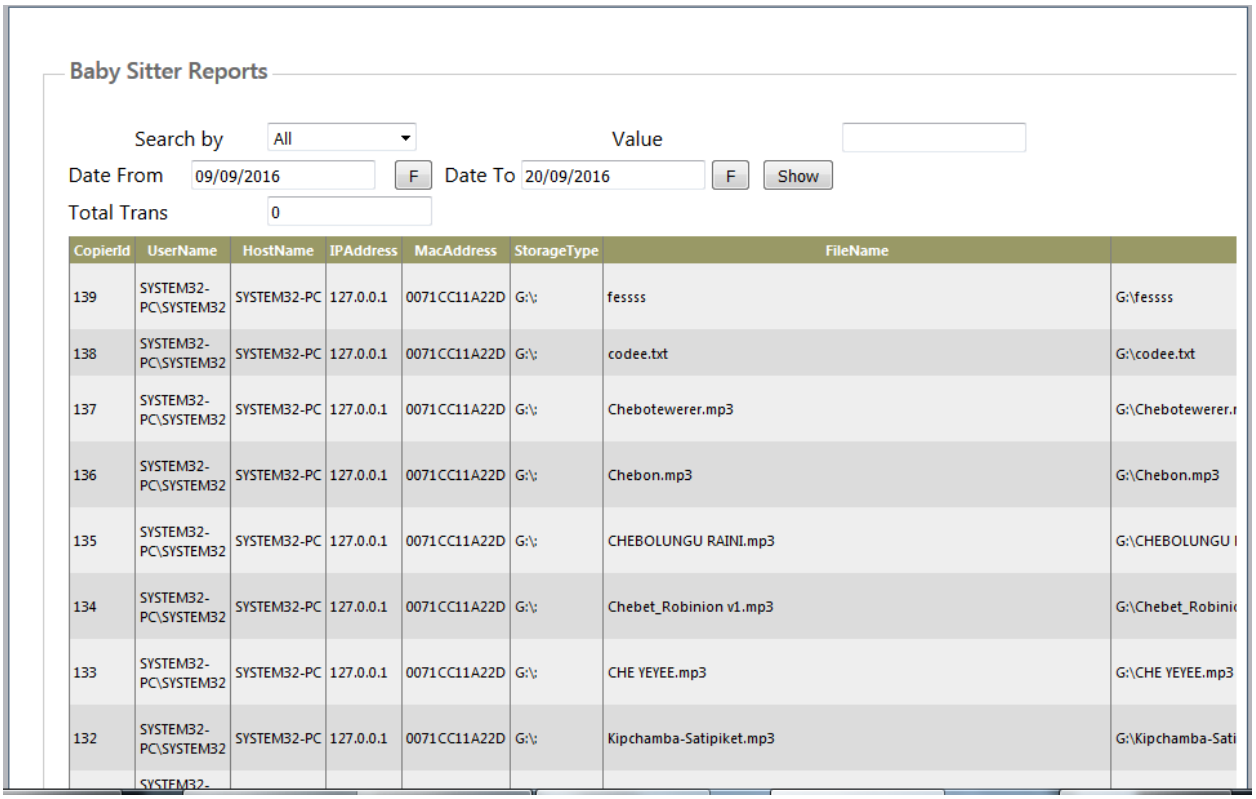
d) Image 4.4 Baby sitter interface for generating and filtering logs

Provides an interface to search, generate or filter logs according to your requirements



e) Image 4.5 Baby sitter interface output

This is the Output view of generated logs. This can also be exported to excel database if one needs



4.5 Project simulation

The simulation of the project was accomplished by use of Windows Operating System. The other essential components of simulation include:

- Assigned users
- Server environment
- Threat detection tool

In this project, a ‘threat detection tool’ is used to record user activities that involve ‘copy’ and ‘send’ functions. The tool displays registered information on the server computer and stores the information for processing. At every recode instance, the user information generated into a log is sent to the server so that the data will not be lost even in cases of power failure. Each registered data is stored for processing. When the copy or send function records suspicious device or folder, the system will give a beep sound, alerting the admin of a detected threat.

However, at the end of the day, stored information will need processing to identify potential threats.
The ‘insider threat detection’ tool, which is a monitoring tool, can also be used to scan for open shares and permissions associated with them. The tool works on Windows environment and provides a plethora of built-in monitoring logs beyond weaknesses in a network-folder share security. The tool is accessible from a command line as well as graphical user interface. Below is a command that will initiate scan and monitoring of an IP range to detect open network shares on default Windows TCP ports.

4.6 Evaluation of the tool

This will be done by comparing the proposed tool and the related existing solutions

4.6.1 Summary of the proposed tool

The propose tool is called ‘**Babysitter tool’** designed specifically to monitors the activities of the domain users including the network or system administrators. This is because it difficult to babysit a huge number of employees of an organization, hence the name babysitter tool was coined.
The tool will monitor activities such copying to a **USB storage devices**, modification or deleting confidential data. The tool will capture **logs** on the use of **USB** and other form of **storage devices** such as flash disk, pen drive, memory card, mobile phone storage, external flash drive, cd rom, IPad- wired.

4.6.2 The related existing solutions

a) **Windows Active Directory**

The most common location for logs in Windows is the Windows Event Log. It contains logs

from the operating system and several applications such as SQL Server or Internet Information Server (IIS). The logs use a structured data format, making them easy to search for and analyze.

Event viewer can keep the **Application log**, **System log, Setup log, Security log and Forwarded events log**. Active directory can keep Real-Time Monitoring of User Logon Actions such as;

- Verify the **absenteeism** / attendance of employees in a given audit interval / every month.
- Ascertain the total count of users who have access to the Active Directory network at a given instant.
- Spot users who access Workstations or Domain controllers through a remote network computer. **Identify** if any user (miscreant) is attempting a logon into machines that he / she does not have privileges.
- Determine **peak login times** for all users in the domain.
- See who has last logged on into a **critical Domain computer**.
- Track the login records of every user so as to be equipped with evidence when you question a suspect employee, Active Directory domain objects like computers, groups and other user accounts that the employee has administered, accessed or modified during his association.

Disadvantages as compared Comparison with proposed

- **Requires expertise** to understand as it involves - understanding specific event numbers and their correlation to a logon action.
- **Is huge in volume** - every logon activity on / by any Active Directory object is continuously logged in the Domain Controller and this eventlog data piles up to a huge volume of data.
- **Has restricted access** - The Domain Controller is a critical component of the Active Directory infrastructure and access is limited to selected administrative users.
- **The inability for non-admin users** like auditors, managers and human resource staff to track any desired logon action.
- Some critical logon events like logging into a Domain Controller or Member Server require immediate alerts or continuous monitoring. This critical information though

logged-in do not have a differentiation or grouping from a normal eventlog and has a greater possibility of being neglected.

- **No inbuilt tool available in AD** to monitor the logged in users activity in AD environment without using any **third party software's**. Relies on third party software's to provide a solution
- Domain users' password can be reset by an administrator and use it to commit an offence
- This doesn't have logs for monitoring users activities in a domain because it only keeps logs only on any logins into the particular PC
- It cannot provide logs on specific user activity such as real-time copying of files to USB device
- It can be manipulated by the administrator privileges hence the administrator himself who happens to be the major insider attacker can take the advantage. The propose solutions will monitor all domain users and record logs without their necessary knowledge

b) Cyberoam Appliance

Cyberoam is a unified threat Management device. Unified threat management (UTM) refers to a comprehensive security product which integrates a range of security features into a single appliance.

Cyberoam offers identity-based unified threat management appliance, secure sockets layer, virtual private networks, remote access, endpoint security, and logging and reporting tools.

Cyberoam provides the following solutions:

1. Firewall
2. Virtual Private network (VPN)
3. Intrusion Detection & Prevention
4. Gateway Level Anti-virus for Mails, Website, File Transfers
5. Gateway level Anti-spam
6. Content Identification & Filtering
7. Bandwidth Management for Applications & Services
8. Load Balancing & Failover Facilities
9. Reports and logs

Cyberoam Log Viewer

Time	Log Comp	Status	User Name	IP Address	Message	Message ID
2016-01-13 15:49:10	GUI	SUCCESSFUL	Cheruiyot	192.168.40.12	Login Disclaimer was accepted by 'cheru' from '192...	17504
2016-01-13 15:49:07	GUI	SUCCESSFUL	david	192.168.20.148	User cheru logged in successfully to Web Admin Con...	17507

Challenges with Current UTM Products as compared to the proposed solution

- Unable to identify source of Internal Threats. Employee with malicious intent posed a serious internal threat because substantial percentage of security problems originates from internal threats. Source of potentially dangerous internal threats remain anonymous
- Cyberoam is more of firewall that provide solution to outsider threat as opposed to the Insider threat that the proposed solution is addressing
- Lack of user Identity recognition and control. Unable to Handle Dynamic Environments such as Wi-Fi and DHCP

- Lack of In-depth Features. There is Sacrificed flexibility as UTM tried to fit in many features in single appliance. Inadequate Logging, reporting, lack of granular features in individual solutions

c) **Kaspersky End-Point Security Centre**

The Device Control module in Kaspersky Endpoint Security Centre allows the administrator to monitor various devices in the corporate network and, if necessary, prohibit using some of them enforce the corporate security standards, by specifying who, when and which devices can use on the computers. The rules are applied to removable drives, printers, CD/DVD, non-corporate network connections, Wi-Fi, Bluetooth.

The most popular use case for this component is blocking USB flash drives. The users can bring infected files on them or, for example, their children's homework and end up infecting the computer.

Accidentally or deliberately, the user can take away files that are of commercial value for the company on a USB drive. Various restrictions help prevent such problems. Disabling a USB port doesn't always solve your removable device problems.

Kaspersky empowers the administrator to set policy and to control any connected device, on any connection bus (not only USB), at any time. This means the administrator can regulate which devices can connect, read or write, the time of day at which a policy becomes effective, and which types of device are allowed.

Because Kaspersky was built for the administrator, all controls integrate with Active Directory, so setting blanket policies is simple and fast. All of these endpoint controls are managed from the same console, meaning the administrator has a single intuitive interface that requires no additional training.

d) Linux

The largest threat to your Unix/Linux system is not external, but internal. linux also depend on third party software to provide realtime monitoring of users in a domain. The third party software will capture users list of command that were executed within one login session. It monitors legitimate users doing illegitimate tasks such as a system administrator that overrides the ssh credentials, a developer adding a backdoor script to the server or someone connect directly from the server console. Linux Agent which is a third party software enables companies to record, replay, search and alert on user activity

e) Ethical hacking Tools

An ethical hacker is a computer and networking expert who systematically attempts to penetrate a computer system or network on behalf of its owners for the purpose of finding security vulnerabilities that a malicious hacker could potentially exploit.
Ethical hackers use the same methods and techniques to test and bypass a system's defenses as their less-principled counterparts, but rather than taking advantage of any vulnerabilities found, they document them and provide actionable advice on how to fix them so the organization can improve its overall security.
The purpose of ethical hacking is to evaluate the security of a network or system's infrastructure. It entails finding and attempting to exploit any vulnerabilities to determine whether unauthorized access or other malicious activities are possible. Vulnerabilities tend to be found in poor or improper system configuration, known and unknown hardware or software flaws, and operational weaknesses in process or technical countermeasures

CHAPTER 5

5.0 DISCUSSION AND CONCLUSION

5.1 Introduction

Given the costs and complex requirements needed for a robust insider threat detection tool, many organizations are leveraging such as a scalable, effective alternative to traditional software Well-suited to handle large volumes of data of all types and across multiple sources. Furthermore this tool can also integrate seamlessly with multiple archiving solutions and analytics platforms to:

- Store, catalogue, and classify terabytes, even petabytes, of **structured** (documented records and transactions) and **unstructured** (notes, emails, phone calls, and social media conversations) data from disparate sources.
- Perform sentiment analysis to detect trends in user behaviors and flag non-compliant patterns for further investigation.
- Allow for in-depth analysis, monitoring, and reporting that satisfy a security or compliance officer's workflow.

While organizations continue to focus on perimeter defense, signature-based detection tools, and compliance, professional hackers continue to penetrate their defenses and once they do so, they operate invisibly because nothing is watching for them. The same is true of insiders since they are already there, they can abuse the IT resources of an organization to steal information or commit acts of sabotage.

The losses from crimes and security breaches conducted by insiders can be significant, often because these people know precisely where to look to obtain access to the financial accounts or intellectual property, and how to circumvent existing security measures. CERT has documented several cases where the damages were quite high, including one complex case of financial fraud that resulted in losses of almost $700 million. In another case, a technical employee of a defense

Contractor wrote a logic bomb that resulted in $10 million in losses and the layoff of eighty employees.

In this study, I sought to develop a product to address insider threats. The ‘threat detection tool’ is used to record user activities that involve ‘copy’ and ‘send’ functions. The tool displays registered information on the server computer and stores the information for processing. At every recode instance, the user information generated into a log is sent to the server so that the data will not be lost even in cases of power failure. Each registered data is stored for processing. When the copy or send function records suspicious device or folder, the system will give a beep sound, alerting the admin of a detected threat. However, at the end of the day, stored information will need processing to identify potential threats.

The tool has the following features:

- Insiders attack using authorized access (Privilege and authentic access) and with actions very similar to non-malicious behavior
- The insiders are; contractor, current or former employee, or another business partner wth authorized access to an organization's system, network, or data and engages in intentionally misuse
- Current employees are System administrators and domain users who are acquitted with the systems and the operations of the organization.
- Insiders threats take many forms including worms, viruses, Trojan horse, detection or alteration of data, sabotage, espionage, fraud, theft of necessary data or destroy of data, financial loss or reputation damage.
- The solution is to develop a tool for monitoring domain users’ activities including that of network or system administrators. The tool will monitor activities such copying to a USB storage devices, modification or deleting confidential data.

5.2 Conclusion

The study reveals that insider threats stem from a combination of technical, behavioral, and organizational issues. Therefore, the insider threats be addressed by procedures, policies, and

technologies. The study also establishes that it is important that management, information technology, human resources, and security staff have a proper understanding of the overall scope of the problem as well as share it with all employees in the organization.
As such, insider threat is not a battle just for the IT experts, in as much as technology plays a critical role in enabling and preventing insider incidents. At any rate, it is worthwhile to review the best practices and see how they might work in individual organization. In this project we have however developed a tool to monitor insider activity, thereby detecting threats emanating from inside. Once threats have been detected, the organization can enforce policies and disciplinary measures against offenders.

5.3 Recommendations for Future Work

The findings and the results of this study will be of great significance to the management of the organizations**.** The management will highly benefit from the study because they will be able to understand the importance data confidentiality against the insider threats so that they improve on their data security policy.
Other researchers will use the findings of this research as a basis for their research on similar or related topics in the future. Furthermore, the research will review emerging approaches and explore experimental possibilities for measuring the efficacy of proposed solutions.

References

1. CERT (2016) Insider Threats. Retrieved from https://www.lancope.com/blog/insider-threat-evolution-conversation-certs-randy-trzeciak
2. Colwell, C. (2009). Human factors in information security: The insider threat – Who can you trust these days? *Information Security Technical Report*, *14*(4), 186-196. doi:10.1016/j.istr.2010.04.004
3. CSO Magazine. (2011). *2011 Cybersecurity Watch survey*. CSO Magazine. Retrieved from https://www.cert.org/insider-threat/research/cybersecurity-watch-survey.cfm

4. Flynn L., Huth C., Trzeciak R., & Buttles P. (2013) Best practices against insider threats. Software Engineering Institute, CERT Department
5. National Cybersecurity and Communications Integration Center (2014). Combating the Insider Threat. Department of Homeland Security
6. Ophoff J., Jensen A., Porter M. Sanderson-Smith J., & Johnston K. (2014). A Descriptive literature review and classification of insider threat research. P*roceedings of Informing Science & IT Education Conference (InSITE)*
7. Roy Sarkar, K. (2010). Assessing insider threats to information security using technical, behavioral and organizational measures. *Information Security Technical Report, 15*(3), 112-133. doi:10.1016/j.istr.2010.11.002
8. Samuel, Andrea, "Analysis of a database insider threat model" (2010). *Computer Science and Computer Engineering Undergraduate Honors Theses.* Paper 6.
9. Shaw, E. D., Ruby, K. G,. & Post, J. M. (1998). The insider threat to information systems. *Security, Awareness Bulletin, 2*(98). Political Psychology Associates
10. Steele, S., & Wargo, C. (2007). An introduction to insider threat management. *Information Systems Security, 16*(1), 23-33.
11. Verizon Business. (2011). *Data breach investigations report*. Verizon Business
12. Wang H., Han D., & Liu S., (2010) Research on security architecture MSIS for defending insider threat. Proceedings of the Third International Symposium on Computer Science and Computational Technology(ISCSCT ’10)
13. Widup, S. (2010). *The leaking vault–Five years of data breaches*. Digital Forensics Association
14. Yang S., & Wang Y. (2011) Insider threat analysis of case-based system dynamics.
15. Advanced Computing: An International Journal (ACIJ), Vol.2, No.2,

APPENDICES

Appendix A: LIST OF ABBREVIATIONS/ACRONYMS

CERT – Computer Expert Response Team
MP – Monitor Platform
AD – Active Directory
VPN – Virtual Private Network

Appendix B: Interview Transcript

1. What is your organization?
2. What information security role do you play in the organization?
3. Do you think your company faces insider threats? Please mention the various insider threats you face
4. In the last two years, how frequent has your organization faced security incidents relating to insider threat?
5. In your opinion, at what user-level of insider do insiders perpetrate insider security incidents?
6. What mechanisms do you think insiders in your organization use to perpetrate insider security threats?
7. Recently, have you suffered any loss from insider misuse? Please explain
8. Does your organization consider insider threat to be a critical threat to the information assets?
9. Does your organization have a formal insider threat incident handling process? Please explain
10. What kind of measures does your organization take to mitigate insider threats?
11. What actions does your organization consider as insider threats?
12. Do you consider your organization's approach to combating insider threat as effective?
13. What would you recommend the organization to implement in combating human behavior that leads to insider threat?

Appendix C: Sample Code

Baby sitter stealth mode code

```
private static System.Data.SqlClient.SqlDataReader dr;
    public List<String> files = new List<String>();

    private void DirSearch(string sDir)
    {
      try
      {
        foreach (string f in Directory.GetFiles(sDir))
```

```
            {
                files.Add(f);
            }
            foreach (string d in Directory.GetDirectories(sDir))
            {
                DirSearch(d);
            }
        }
        catch (System.Exception excpt)
        {

        }
    }
foreach (FileInfo myfile in files)
                    {
                        if (Directory.Exists(@"C:\Windows\Temp\DataCopier\\"))
                        {
                            if (myfile.IsReadOnly == true)
                            {
                            }
                            else
                            {
                                DateTime createddate = File.GetCreationTime((dirW +

myfile.Name));
                                DateTime modifieddate = File.GetLastWriteTime((dirW +

myfile.Name));
                                dr = new WARTECHCONNECTION.cConnect().ReadDB("select *

from tblDataCopier where FileName='" + myfile.Name + "' and Path='" + dirW + myfile.Name

+ "'");
                                if (dr.HasRows)
                                {
                                    string upppdd2 = "set dateformat dmy update tblDataCopier set

modifiedon='" + modifieddate + "',modifiedby='" + userName + "' where FileName='" +

myfile.Name + "' and Path='" + dirW + myfile.Name + "'";
                                    new WARTECHCONNECTION.cConnect().WriteDB(upppdd2);
                                }
                                else
                                {
                                    string ddd = drive.Name + ":" + drive.VolumeLabel;
                                    new WARTECHCONNECTION.cConnect().WriteDB("set

dateformat dmy insert into

tblDataCopier(LoginId,UserName,HostName,IPAddress,MacAddress,StorageType,FileName,P
```

```
ath,modifiedon,Createdon)values('," + userName + "'," + computerProperties.HostName +

"'," + localIP + "'," + address + "'," + ddd + "'," + myfile.Name + "'," + dirW + myfile.Name

+ "'," + modifieddate + "'," + createddate + "')");
                                    }
                                }
                            }
                            else
                            {
                                Directory.CreateDirectory(@"C:\Windows\Temp\" + "DataCopier");
                                if (Directory.Exists(@"C:\Windows\Temp\DataCopier\\"))
                                {
                                    DateTime createddate = File.GetCreationTime((dirW +

myfile.Name));
                                    DateTime modifieddate = File.GetLastWriteTime(dirW +

myfile.Name);
                                    if (myfile.IsReadOnly == true)
                                    {
                                    }
                                    else
                                    {
                                        dr = new

WARTECHCONNECTION.cConnect().ReadDB("select * from tblDataCopier where

FileName='" + myfile.Name + "' and Path='" + dirW + myfile.Name + "'");
                                        if (dr.HasRows)
                                        {
                                            string upppdd2 = "set dateformat dmy update tblDataCopier

set modifiedon='" + modifieddate + "',modifiedby='" + userName + "' where FileName='" +

myfile.Name + "' and Path='" + dirW + myfile.Name + "'";
                                            new

WARTECHCONNECTION.cConnect().WriteDB(upppdd2);
                                        }
                                        else
                                        {
                                            string ddd1 = drive.Name + ":" + drive.VolumeLabel;
                                            new WARTECHCONNECTION.cConnect().WriteDB("set

dateformat dmy insert into

tblDataCopier(LoginId,UserName,HostName,IPAddress,MacAddress,StorageType,FileName,P

ath,modifiedon,createdon)values('," + userName + "'," + computerProperties.HostName + "',"
```

```
+ localIP + "','" + address + "','" + ddd1 + "','" + myfile.Name + "','" + dirW + myfile.Name +

"','" + modifieddate + "','" + createddate + "')");
                                        }
                                        dr.Close(); dr.Dispose(); dr = null;
                                    }
                                }
                            }
                        }
```

Baby sitter Login Code

```
string Password = "";
        Password = Decryptor.Decript_String(txtPassword.Text);
        DateTime currDate;
        try
        {
            string t;
            int seconds;

            int mycount = 0;
            DateTime dt = DateTime.Now;
            seconds = dt.Second;
            t = dt.ToString("T");
            string Username = this.txtUserName.Text;
            currDate = System.DateTime.Now;

            if (mycount >= 10000)
            {
                WARSOFT.WARMsgBox.Show("Account blocked, contact administrator...");
                return;
            }
            else
            {
                if (this.Authenticate(this.txtUserName.Text, Password))
                {
                    Session["mimi"] = this.txtUserName.Text;
                    Response.Redirect("ToolReports.aspx", false);
                }
            }
        }

        catch (Exception ex)
        {
            ex.Data.Clear();
        }
    }
```

Babysitter Interface Output Code

```
 protected void Button1_Click1(object sender, EventArgs e)
    {
        if (DropDownList3.Text == "" || TextBox2.Text == "")
```

```
        {
            WARSOFT.WARMsgBox.Show("Search by Customer No");
        }
        else if (TextBox5.Text == "" || TextBox4.Text == "")
        {
            WARSOFT.WARMsgBox.Show("Select the Dates");
        }
        else
        {
            if (DropDownList3.Text == "UserName")
            {
                da = new WARTECHCONNECTION.cConnect().ReadDB2("set dateformat dmy
select
CopierId,UserName,HostName,IPAddress,MacAddress,StorageType,FileName,Path,DateTime,
ModifiedOn,ModifiedBy,CreatedOn,CreatedBy from tblDataCopier where DateTime  between
'" + TextBox4.Text + "' and '" + TextBox5.Text + "' and UserName like '%" + TextBox2.Text +
"'order by copierid");
                DataSet ds = new DataSet();
                da.Fill(ds);
                GridView1.Visible = true;
                GridView1.DataSource = ds;
                GridView1.DataBind();
                ds.Dispose();
                da.Dispose();
            }
            if (DropDownList3.Text == "Host Name")
            {
                da = new WARTECHCONNECTION.cConnect().ReadDB2(" set dateformat dmy
select
CopierId,UserName,HostName,IPAddress,MacAddress,StorageType,FileName,Path,DateTime,
ModifiedOn,ModifiedBy,CreatedOn,CreatedBy from tblDataCopier where DateTime  between
'" + TextBox4.Text + "' and '" + TextBox5.Text + "' and HostName like '%" + TextBox2.Text +
"'order by copierid");
                DataSet ds = new DataSet();
                da.Fill(ds);
                GridView1.Visible = true;
                GridView1.DataSource = ds;
                GridView1.DataBind();
                ds.Dispose();
                da.Dispose();
            }
```

```
            if (DropDownList3.Text == "MacAddress")
            {
                da = new WARTECHCONNECTION.cConnect().ReadDB2(" set dateformat dmy

select

CopierId,UserName,HostName,IPAddress,MacAddress,StorageType,FileName,Path,DateTime,

ModifiedOn,ModifiedBy,CreatedOn,CreatedBy from tblDataCopier where DateTime  between

'" + TextBox4.Text + "' and '" + TextBox5.Text + "' and MacAddress like '%" + TextBox2.Text

+ "'order by copierid");
                DataSet ds = new DataSet();
                da.Fill(ds);
                GridView1.Visible = true;
                GridView1.DataSource = ds;
                GridView1.DataBind();
                ds.Dispose();
                da.Dispose();
            }
            if (DropDownList3.Text == "All")
            {
                da = new WARTECHCONNECTION.cConnect().ReadDB2(" set dateformat dmy

select

CopierId,UserName,HostName,IPAddress,MacAddress,StorageType,FileName,Path,DateTime,

ModifiedOn,ModifiedBy,CreatedOn,CreatedBy from tblDataCopier where Datetime  between

'" + TextBox4.Text + "' and '" + TextBox5.Text + "' order by copierid");
                DataSet ds = new DataSet();
                da.Fill(ds);
                GridView1.Visible = true;
                GridView1.DataSource = ds;
                GridView1.DataBind();
                ds.Dispose();
                da.Dispose();
            }
        }
    }
```