
**JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY**

# THE LATEST CYBERCRIME TRENDS IN KENYAN LEARNING INSTITUTIONS

**By**

**OPIYO OCHIENG' RAY**

**ADMISSSION NUMBER: I132/0860/2013**

**SUPERVISOR**

**MR. PAUL ABUONJI**

**A project report submitted to School of System Innovative and Informatics in partial fulfillment for the award of the Degree of Bachelor of Computer Security and Forensics in Jaramogi Oginga Odinga University of science and technology.**

**December 2016**

## DECLARATION

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

Sign: _____ Date: _____

Opiyo Ochieng' Ray

This work has been submitted for examination with my approval as University Supervisor.

Sign: _____ Date: _____

Mr. Paul Abuonji

## DEDICATION

I dedicate this project with much love and appreciation to my family members. I owe gratitude to the Almighty God.

## ACKNOWLEDGEMENTS

I thank the Almighty God for giving me life and strength during the entire process, my supervisor Mr. Paul Abuonji for sparing his valuable time to guide and ensure that the project was successfully completed. I wish to acknowledge my friends and my classmates for their encouragement. Special thanks to Mr.Olala Samwel for his mentorship, my dear Miss. Onyango Jackline for her advice and support and my parents for financial support and spiritual empowerment to ensure that the entire process is done successfully. Not forgetting all my lecturers for their devoted time during my learning period. May the gracious God bless you abundantly. To all the readers of this document, God bless you too.

# TABLE OF CONTENTS

## Contents

## LIST OF TABLES

## LIST OF FIGURES

## ACRONYMS AND ABBREVIATIONS

WI-Fi- Wireless Fidelity.

ERP – Enterprise Resource Planning.

VoIP – Voice over Internet Telephony.

IP – Internet Protocol.

ISACA – Information Systems Audit and Control Association.

IM- instant messaging.

FBI - Federal Bureau of Investigation.

VP- Vice President.

FIDO- Fast- Identity Online.

ODPP- Office of the Director of Public Prosecutions.

USD- United State Dollar.

KES - Kenyan Shillings.

TESPOK -Telecommunications Service Providers Association of Kenya.

USA – United States of America.

ICT - Information and Communication Technology.

ISPs - Internet Service Providers.

CID - Criminal Investigation Department.

CCK -Communications Commission of Kenya.

IT – Information Technology.

CCSMM - Community Cyber Security Maturity Model.

DoS - Denial-of-service.

AETs - Advanced Evasion Techniques.

DLP - Data Loss Prevention.

HTML – Hyper-text Make-up Language.

JOOUST – Jaramogi Oginga Odinga University of Science and Technology.

NGOs – Non-Government Organisations.

PCs – Personal Computers.

IXP - Internet Exchange Point.

E-laws – electronic laws.

E-commerce – Electronic Commerce.

SMEs – Small and Medium Enterprises.

USB – Universal Serial Bar.

CD – Compact Disc.

DVD – Digital Versatile Disc.

## ABSTRACT

With the rapid globalization of the Kenyan economy, learning institutions are faced with the ever changing competitive environment full of cybercrime challenges. Of late there have been serious cases on hacking of various departments within the institutions in search of confidential information for alterations such as institutions of higher learning in Kenya are now feeling the heat of cybercrime as students target their databases. This has become a shocking issue in most of the institutions. Most students have become malicious as they intend to alter some of the key details such as information recorded in the transcripts, financial information i.e. alteration of fee balances, and even some of the confidential information regarding the set-up of various faculties within the universities.

This study focused on the following objectives to ensure that the set up goals are achieved. The main objective of the study was to investigate the prevalence of cybercrime activities against Kenyan learning institutions and recommend possible solutions. This was linked to the following specific objectives; to explore how the latest cybercrime trends affect Kenyan learning institutions, to identify measures put in place by the institutions of higher learning institutions to mitigate against these cybercrimes activities and finally to investigate how the institutions engage with authorities and regulators to address cybercrime.

Mixed methods research methodology has been used in this study as it involved the collection of both qualitative and quantitative data. Mixed methods research refers to the use of data collection methods that collect both quantitative and qualitative data. Mixed methods research acknowledges that all methods have inherent biases and weaknesses; that using a mixed method approach increase the likelihood that the sum of the data collected will be richer, more meaningful, and ultimately more useful in answering the research questions. In line with this the following were used as data collection tools; primary sources of data, secondary sources of data survey that implied the use of structured questionnaires with both open ended questions and closed questions. All data was analyzed with the use of likert-scale and Microsoft excel tools.

The outcomes presented in tables and bar graphs basing on issues that were involved in the study. The research has great demarcations that should be addressed in time to control the effects of cybercrime activities in various institutions.

## CHAPTER 1:

### 1.0 INTRODUCTION

The general definition of cybercrime may be unlawful actions where the computer is used as a tool, a target or both that threaten a nation's security and financial health. (Chavan F. al, 2010). Both governmental and non-governmental criminals engage in cybercrimes ranging from espionage, financial theft and other cross border crime. Simply, cybercrime refers to any criminal activity carried out with the aid of a computer system. The term cybercrime can also be defined as an act committed or omitted in violation of a law forbidding or commanding it and for which punishment is imposed upon conviction. Other words represents the cybercrime as Criminal activity directly related to the use of computers, specifically illegal trespass into the computer system or database of another, manipulation or theft of stored or on-line data, or sabotage of equipment and data. (Halder & Jaishankar, 2011).

### 1.1 Background Information of the Study

Cybercrime has become a major issue in most the Kenyan organisations. The problem comes due to high increase in the number of internet users as has been shown in various researches. It is real that the number of internet users is increasing at high rate. According to the late internet usage report from Communication Authority of Kenya there were estimated 26.1million internet users in Kenya as of December 2014. This is about 64% of country's total population with access to the internet and over 70% being below 25 years (Serianu, 2015).

As communities embrace information technology for efficient service delivery, the bad elements in the society are constantly exploiting the same technology for illegitimate gains. Criminals are exploiting the Internet and other networks to advance the illegal business. As result, cybercrime is on the increase. Just as technology is advancing, cyber-attacks are getting more sophisticated. (Poonia, 2014).

The Internet structure lacks a single central control. Therefore, anyone connected online can carry out legitimate or malicious tasks. Cybercrimes exploit this unstructured nature of the Internet. In addition, individuals with expertise on programming and other complicated computing skills are the majority involved in compromising the security of the computer users currently, there are many online tools that are misused. Software developers who contravene

software engineers' professional code of ethics (Summerville, 2011) can be cited as the source of cyber-attacks. The primary target of most reported cybercrimes in Kenya in 2014 targeted key government institutions' websites. Successful cyber-attacks in Kenya are blamed on poor detection tools and a lack of capacity to address the crime.

It is common norm in the country that, there is high number of technology dependence and thus results to high number of cyber criminals. The higher the number of technology dependence the greater the number of the cyber criminals. This comes due to the several attack sites that are created with the larger number of the technology dependence. Every organization tend to go online in their services i.e. cloud computing this majorly practiced in the Kenyan institutions as most of them embrace e-learning programmes. The question remains, how safe is the platform? Once this question is answered then the problem of cyber-attacks likely to be solved.

The study reveals that with this high percentage of internet users, it is quite stressing that the number of security professionals remains dismal and unable to match the entire population's percentage that uses the internet. (Serianu 2015).

According to ISACA Kenya there are 1000 certified ICT risk professionals in the market. This means there is approximately 1 security professional for every 200 000 internet users. This is worrying ratio that needs to change if we are going to successfully secure the cyber space in Kenya. By the year 2017 it is estimated mobile broadband subscription will approach 80% of the country's total population. By the year 2020 the number of network devices "internet of things" will outnumber people by six to one, transforming current conceptions of the internet. It will become hard to imagine a non-computer crime and perhaps any crime. (Serianu 2015)

Kenyan learning institutions are vulnerable to various cyber-attacks such as data exfiltration, social engineering, insider threats, Database breaches poor identity and access management, inadequate budget and poor management support, emerging technology complications and ERP automation problems.

Besides these the following have been found as the major motivations to cybercrime activities in Kenya:

Lack of legislation touching on cyber-attacks. This is due to poor detection techniques-mechanisms of tracking the culprit which are much behind. Lack of capacity to respond to the crime- this exposes vulnerability of systems in Kenya. Attackers are also capitalizing on the naivety of some of the Internet system users i.e. numerous "mouse click events" without thought of what is likely to happen next. Solution to every problem begins from analysis of consequences. This ought to be the case for Cyber security. (International Journal of Education and Research, 2015).

The study has clear explanation on the mentioned cyber-attacks, how they pose danger to Kenyan learning institutions. The research is based on finding trusted control measures to ensure that all the problems are solved or fully subdued, prevented and even eradicated. The research study is therefore focused on the Kenyan learning institutions in general, both private and public ones such as universities, colleges, and schools.

**1.2 Problem statement.**

There have been serious cases of cybercrime attacks that have been launched in most of the Kenyan organizations especially the learning institutions. The attacks can be classified as; old or current and this data can be used to predict future trends in cybercrime. The latest report on cybercrime shows that the cyber-attacks that are launched in various learning institutions are categorised as: cyber stalking, data exfiltration, Denial of service attack, identity theft, data interception, data theft, network interference, access crimes such as; unauthorised access, virus dissemination among others. Due to these attacks, Kenyan learning institutions have incurred serious economical and service delivery loses. Most institutions have reported cases on loss of confidential information, alteration of certain information such as change on student's fee balances and change of grades. In regard to these I have been able to come up with a research to bring out what is likely to be done to save the learning institutions from such cybercrime activities. Due to this research has been able to come up with clear information on how the stated cybercrime trends can be controlled, eradicated or reduced. This likely to be achieved by showing: what the institutions' management personnel should do in saving the learning institutions from the effects of such activities.

## 1.4 Objectives of the Study.

### 1.4.1 Overall Objective.

1. To investigate the prevalence of cybercrime activities against Kenyan learning institutions and recommend possible solutions.

### 1.4.2 Specific Objectives.

1. To explore how the latest cybercrime trends affect Kenyan learning institutions.

2. To identify measures put in place by the institutions of higher learning to mitigate against these cybercrimes

3. To investigate how the institutions engage with authorities and regulators to address cybercrime.

## 1.5 Research Questions.

1. What are the main cybercrime that have been dated as the latest attacks in Kenyan learning institutions?
2. What are the kind of measures have been put in place to address cybercrimes trends towards Kenyan learning institutions?
3. How have the institutions engage with authorities and regulators to address cybercrime?

## 1.6 Importance of the Study.

The study is entitled in providing evidence for development of cybercrime policy and regulatory framework that acknowledges and considers cyberspace violence against the learning institutions in Kenya and creates awareness on cybercrime activities to the institutions' managers. The study is therefore of importance to the government, governmental agencies, especially the learning institutions.

## 1.7 Scope of the Study.

The study is contextual. The study restricts itself to cyber world. It reviews crimes that originate from the world and taken to the cyber, and new ones entirely originating from the cyberspace.

## 1.8 Justification of the Study.

The study shows the latest cybercrime trends in the various learning institutions and gives clear definition on how such crimes are conducted.

It is true as the research reveals greater percentage of Kenyans are not aware of what cybercrimes are, some attacked and never give reports on various attacks, some are too down to tell what kind attacks have been experienced in their institutions. It is categorized that; 86% of the internet users are aware that cybercrime is real, 33% don't apply any risk management, and 98% of the government organizations are convinced that they are protected from cyber-attacks internally while 94% of the government organizations are not protected from external attacks (Serianu, 2015). The study has strategies to go about the problems on cyber-attacks.

Most of the problems that are hitting Kenyan learning institutions originate from cyber-attacks. The study should alert the nation on the top local vulnerabilities that can be of great loss when fully utilized by cyber criminals. Top attack ports i.e. (port 5060 SIP) was the mainly targeted port by attackers emphasizing the need to secure VoIP and IP telephony solutions. The study should attain Kenya cyber-intelligence report that has been recently recorded.

Some of the common cybercrime trends in Kenya that are likely to be discussed in this research are:

### Malware

Malware refers to malicious software that finds their way to a computer system especially from the Internet. They could be viruses, trojans worms, and other software that get installed in a computer without the user's knowledge. In several cases, the software will pretend to be legitimate software. Malware's intentions are diverse ranging from spying on your work, phishing or sniffing password, monitoring web sites visited access to confidential data, and denial of service, among others. (Cybercrimes on the rise in 2015).

## Identity theft or Fraud

Cybercriminals obtain personal and confidential data belonging to someone or an institution they are targeting. This information can be obtained through social engineering, email phishing, purchase the data on the black market, or use tools and techniques to search. A majority of personal data is the open access in the Internet especially in this era of socializing sites. An attacker may befriend a non-suspecting individual and obtain all the information they needed to launch an attack or entice them to perform some action. (Cybercrimes on the rise in, 2015).

Identity theft typically succeeds when a cybercriminal gets an individual's personal identification information. The crime is motivated by the likely financial reward or corruption done on accessed data. Therefore, identity theft is a gateway for fraud cases such as credit-card fraud and other related cases. (Cybercrimes on the rise in, 2015).

## Cyber stalking

Simply defined, cyber stalking is the use of technology to harass someone. An attacker harasses a victim using electronic communication, such as e-mail, instant messaging (IM), phone calls or posting messages on chat forums or discussion groups or social sites. A cyber stalker will hide in the Internet for anonymity to avoid detection. The stalker relies upon the anonymity afforded by the Internet to allow them to stalk their victim without being detected. The messages sent range from sexual harassment, threats to one's security and safety, posting of false information for defamation or just annoying attention to an individual's private life and family activities. Unlike general cyber harassment, cyber stalking poses a credible threat to the victim. In Kenya cyber stalking takes many forms such as defamation or libel, falsification, fraud, intimidation, offensive comments, personal attacks, graphic violence and violation of rights to privacy. (Cybercrimes on the rise in 2015).

## Ransomware

Ransomware built from two words, ransom and malware it's a kind of malware attack that demands payment in exchange of stolen computer functionality. Most attacks of this nature make use of encryption as means of extortion. Basically encrypting files on computer's hard drive and then asking for financial favours to decrypt them back for the victim to have them back. It's a

form of denial of service attack .A majority of the people will go dramatic lengths in order to access locked information or to prevent sensitive information from being leaked to the public. Ransomware is a crime in the rise and it's projected as the favorite cybercrime of the future (cybercrimes on the rise in 2015).

Settling on the latest cybercrime trends in Kenyan learning institutions, should give clear definition on certain cyber criminals into details as they are categorized:

**Crackers**: These individuals are intent on causing loss to satisfy some antisocial motives or just for fun. Many computer virus creators and distributors fall into this category.

**Hackers**: These individuals explore others' computer systems for education, out of curiosity, or to compete with their peers. They may be attempting to gain the use of a more powerful computer, gain respect from fellow hackers, build a reputation, or gain acceptance as an expert without formal education.

**Pranksters**: These individuals perpetrate tricks on others. They generally do not intend any particular or long- lasting harm.

**Career criminals**: These individuals earn part or all of their income from crime, although they malcontents, addicts, and irrational and incompetent people: "These individuals extend from the mentally ill do not necessarily engage in crime as a full-time occupation. Some have a job, earn a little and steal a little, then move on to another job to repeat the process. In some cases they conspire with others or work within organized gangs. (The FBI reported, 1995).

### 1.9 The Study Limitations.

**1.9.1 Problems of security:** Various sites over the internet are not properly secured to ensure that all internet users are safe whenever they make an access. The research does not involve key details on security side as compared to the attack cases.

**1.9.2 Wrong assumption:** it is assumed that most Kenyans are aware of cybercrime attack; the study only tackles very small area on that.

**1.9.3 Lack of awareness:** cybercrime is real that enquires all the employees be aware on the latest cases on that. This research is not meant for creating the necessary awareness.

The study is limited to learning institutions. Main focus is directed to universities, colleges, and schools. The relevancy of the study revolves around latest cybercrime trends in such institutions. The time frame is taken in five years down the line i.e. the study only reflects matters that have been discovered from 2012 to 2016.

# CHAPTER 2

## 2.0 LITERATURE REVIEW.

### 2.1 Introduction

This chapter reviews literature related to the study objectives based on the latest cybercrime in Kenyan learning institutions; Literature review seeks to bring out the existing body of knowledge relevant to cybercrime and learning institutions, critic the work and identify gaps. These gaps motivate the study to advance the body of knowledge on cybercrime and the learning institutions.

According to Alice Munyua, the literature review should illustrates the work undertaken in the area of cybercrime and learning institutions and the measures taken to address the vice as a deterrent to safeguard use of cyberspace by such institutions. To get a deep insight in this area, the literature review sheds insight on the features of perpetrators of cybercrime, the victims of cybercrime, and the environmental features that foster the commission of the crime and, finally the strategy and measures being taken to address the vice. Cybercrime is an area of interest and therefore widely addressed by many scholars and stakeholders. (Munyua, 2007).

### 2.3 Review of Past Studies in the Area

According to Robert Capps, (VP Business Development, and Data Security). In his posting, Sidestepping the Threat Posed by Breached Data, Capps explains that efforts to value data will be the most impactful actions an organization can take to reduce the number, scope and impact of breaches that lead to cybercrime.

In the special guest posting, Cyber Criminals are Automating - Why Can't We?, by (Jonathan Sander), VP of Product Strategy, Lieberman Software, the question posed in the title is a great one. As the world moves to multi-factor authentication, and hopefully the elimination of passwords through industry efforts such as the FIDO Alliance, the automation of password protection in the meantime just makes common sense. After all, as Sander points out, hackers can attempt to use millions of password combinations in seconds thanks to today's computing power. (VP of Product Strategy, Lieberman Software).

According to Leiner et.al, internet forms an open forum for the sharing of information as it involves collaboration many individuals. In line with the organization's activities that are shared online, they are easily interrupted, this may be conducted by hackers i.e. diversion of online transaction and even alteration of confidential data in on online sharing among the organizations. (Leiner et.al. 2009)

As the internet and ICT provides new prospect for government and business to operate and increase their presence, ICT also present opportunities for those with criminal intention and leaves individuals, communities, organisations and nations, highly exposed to the threat of cyber-attack. (Choo, 2011)

According to this, (Julisch 2013) has identified four anti-patterns that undermine the cyber security of organisations. These include: an overreliance on institution to make security decisions, where decisions-makers generally rely on their institution and experience often fraught with cognitive-biases; leaving cracks in the security foundation, where organization continue to rely too much on the relatively static knowledge within products and finally; weak governance, characterized by unclear decisions rights and processes, creating systemic control gaps and vulnerabilities. (Julisch, 2013)

Cybercrime majorly conducted on the cyberspace and due to this, according to (Schreier 2012) believes that the internet openness caries downsides in that, it makes it easier to attack application and operating systems that are not adequately defended. In this regard establishing and conforming the identity of attacker online can be a tedious process. Most of the Kenyan organizations undergo such consequences as they tend to go online in terms of their services. Banks are seriously affected in this area compared to learning intuitions. (Schreier, 2012)

The Cybercrime Bill is an initiative of the Office of the Director of Public Prosecutions (ODPP). It seeks to equip law enforcement agencies with the necessary legal and forensic tools to tackle cybercrime, which is said to have cost nearly KES 2 billion (USD 23 million) to the Kenyan economy in 2013. The Bill comes on the heels of a Cyber Security conference in June 2014 where the Telecommunications Service Providers Association of Kenya (TESPOK) and cyber security groups from Canada, Singapore, South Africa, India and USA discussed the role of the private sector in tackling cybercrime. The meeting recommended the adoption of a comprehensive cybercrime law in light of the perceived failings the existing legal framework in

dealing with recent terrorist attacks. Kenya: (Cybercrime and Computer Related Crimes Bill, 3:44)

The identification of Information and Communication Technology (ICT) as an essential tool for sustainable development has proved to be worth every investment. As a result of this, Internet usage in Kenya has grown rapidly resulting in the explosion of Internet Service Providers (ISPs) and Internet access points. A case study conducted on the impact of Cybercrime on security in Kenya, Nairobi as the case study it was found that thirty one (31) out of the fifty one (51) responded giving a response rate of 60.78% percent. It was found that the Cybercrime is prevalent in Nairobi although largely unreported. To a great extent, it was discovered that Internet Service Providers had established basic measures in order to curb the growing cyberspace crimes; as spamming activities remain prevalent in Kenya. Also, to a great extent the Criminal Investigation department (CID) and Communications Commission of Kenya (CCK) have recognized that cybercrime is a growing threat to security in Nairobi and have collaborated with ISP's to implement measures. (Effects of Cybercrime on State Security, 2011).

Cyber security plays an important role in the ongoing development of information technology, as well as Internet services. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being. Making the Internet safer and protecting Internet users has become integral to the development of new services as well as government policy. Deterring cybercrime is an integral component of a national cyber security and critical information infrastructure protection strategy. In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures. At the national level, this is a shared responsibility requiring coordinated action related to prevention, preparation, response and recovery from incidents on the part of government authorities, the private sector and citizens. At the regional and international level, this entails cooperation and coordination with relevant partners. Understanding cybercrime: (Phenomena, 2014).

According John Walubengo faculty Dean at Multimedia University report that with the growing internet connectivity in the country, local universities, Kenya Police and IT training firms are turning to security firms for hands-on-experience in fighting cybercrime. The Kenyatta University, KCA University, Computer Pride and Techno Brain have partnered with EC, an American security firm to equip their students in detection, investigation of cybercrime. (Report 5th. March. 2012).

A gentle reminder by the Official ISC( On Demand Training and The Rise of the Cloud Security Professional Whitepaper) states that the Cyber Security Trend home page has been designed as your easy to use gateway to valuable resources. This includes feature articles; news, white papers and profiles of certifications that can help you keep your organization safe and secure and help advance your career. There are just two of several great resources available for downloading and review. In addition the companion Cloud Security Resource site is also a source of valuable security insights and news. (Whitepaper, 2011).

Per the third posting from special guest Arthur Braunstein, vice president of Strategic Accounts, (Morphisec, Cyber Security: Method or Madness?), should be of particular interest because of the perspective presented. As an inducement to read the entire article, his conclusions should encourage readers as to how he got there. He explains, "It does not make sense to get better at doing more of what already isn't working. Moving Target Defense solves the problem of sophisticated attacks by making the attackers' targets unfindable. Without the need to detect an attack, the cost and effort of defense plummet at the same time success rockets up. And without a target, attacks evaporate. For the defenders, it's a game changer. For the attackers, it's game over. Method 100%. Madness 0%."(Special guest Arthur Braunstein**)**

John Herhalt (Cybercrime – a growing challenge for governments) states that in a digital age, where online communication has become the norm, internet users and governments face increased risks of becoming the targets of cyber-attacks. As cyber criminals continue to develop and advance their techniques, they are also shifting their targets — focusing less on theft of financial information and more on business espionage and accessing government information. To fight fast-spreading cybercrime, governments must collaborate globally to develop an effective model that will control the threat. (Monitor, July 2011).

(Monitor, July 2011). Asserts that advancements in modern technology have helped countries develop and expand their communication networks, enabling faster and easier networking and

information exchange. Currently, there are nearly 2 billion internet users and over 5 billion mobile phone connections worldwide. Every day, 294 billion emails and 5 billion phone messages are exchanged. Most people around the world now depend on consistent access and accuracy of these communication channels. The growing popularity and convenience of digital networks, however, come at a cost. As businesses and societies in general increasingly rely on computers and internet-based networking, cybercrime and digital attack incidents have increased around the world. (Monitor, July 2011).

In line with Lockheed Martin and NASA comment, over the past few years, the global cybercrime landscape has changed dramatically, with criminals employing more sophisticated technology and greater knowledge of cyber security. Until recently, malware, spam emails, hacking into corporate sites and other attacks of this nature were mostly the work of computer 'geniuses' showcasing their talent. These attacks, which were rarely malicious, have gradually evolved into cybercrime syndicates siphoning off money through illegal cyber channels. By 2010, however, politically motivated cybercrime had penetrated global cyberspace. (Phenomena, 2014).

Concerning the report given by Fredrick Mugambi Muthengi Department of Computer Science Chuka University on combating current and emerging cybercrimes in Kenya (2011) he mentions that Companies start a common platform for sharing cybercrime information. This sharing would increase preparedness and help in collaborative efforts to combat cybercrimes in their various evolving forms. As such, it is important that companies embrace a multi-faceted approach on dealing with cybercrime. The public and the private sector need a common ground to tackle this menace by devoting more resources to secure cyber space. (Muthengi, 2011).

Invest heavily on computer network security: specialized training for system administrators; crime awareness forums in learning institutions especially universities; encourage computer and Science and IT students to undertake specific lecturer or researcher coordinated teamwork projects on cyber security – securing software systems. The Community Cyber Security Maturity Model (CCSMM) was proposed to help communities establish viable and sustainable cyber security programs. (Cybercrimes in Kenya, 2011).

## 2.3 Conceptual Framework

The main variables are the perpetrators, the victims, the environmental factors and a strategy to address the vice and its impact on the learning institutions in Kenya. Figure 1 illustrates the interrelations of the variables.

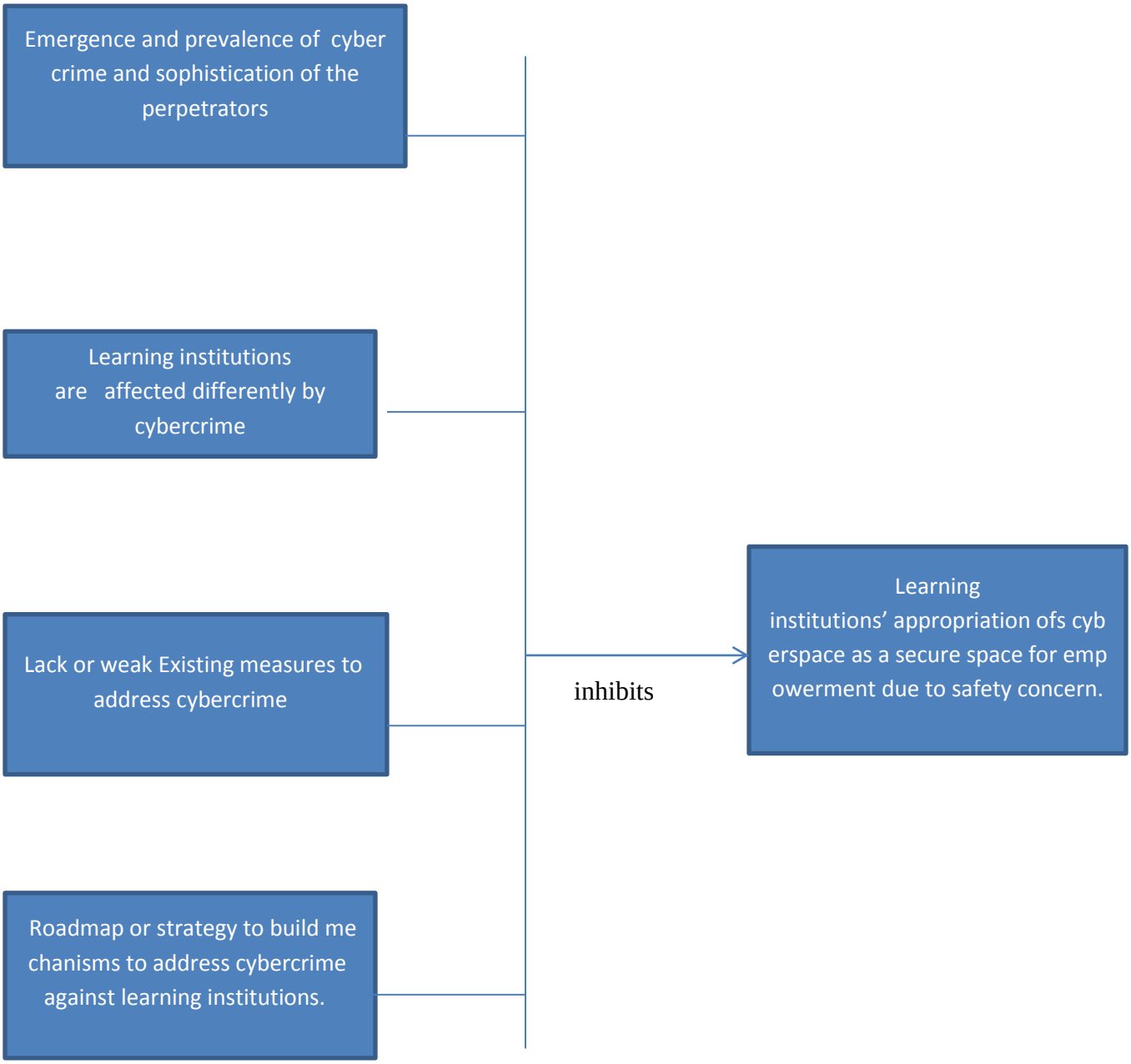



**Fig 1: Interrelationships of variables on cybercrime and Learning institutions.**

**Fig1.1 showing the sophistication of attack tools against the required knowledge of the attackers.**

### 2.4 Tools of Perpetration.

Cyber stalkers use increasingly sophisticated means to target and harass their victims using websites, chat rooms, discussion forums, open publishing websites (e.g. blogs) and email. There are three primary ways in which cyber stalking is conducted:

• Email Stalking: Direct communication through email.

• Internet Stalking: Global communication through the Internet

• Computer Stalking: Unauthorized control of another person's computer.

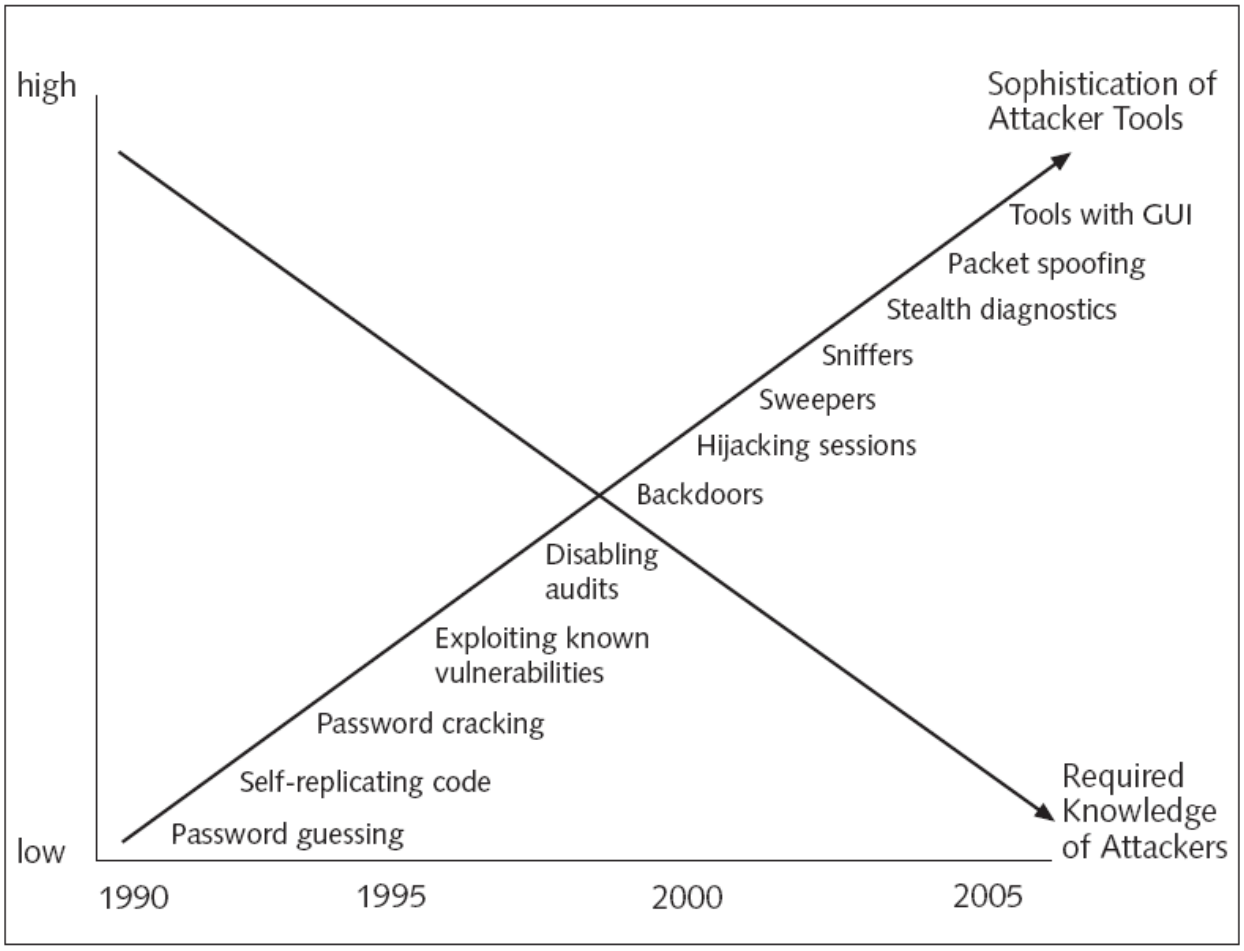



**Figure 1-1** Increased sophistication of attack tools

### 2.4.1 Difficulties in defending against attacks include the following:

Speeds of attacks now faced with zero-day attacks- attackers are very first in their activities.

Greater sophistication of attacks – most of the attacks have become sophisticated and complex in nature.

Simplicity of attack tools – most of the attacking tools are simple and easily obtained by any interested persons on line.

Attackers can detect vulnerabilities more quickly and more readily exploit these vulnerabilities

Delays in patching hardware and software products – this has left most of the attacker's targets more vulnerable and easily attacked.

Most attacks are now distributed attacks, instead of coming from only one source they come from many sources.

As communities embrace information technology for efficient service delivery, the bad elements in the society are constantly exploiting the same technology for illegitimate gains. Criminals are exploiting the Internet and other networks to advance the illegal business. As result, cybercrime is on the increase. Just as technology is advancing, cyber-attacks are getting more sophisticated. The fast growth in cyber security challenges requires a robust framework to address the menace. Poor or no cyber safety measures lead to massive loss of critical data and financial assets. (Poonia, 2014).

Security is a primary and widespread concern for software systems especially web-based software systems. The ease of performing cyber-attacks has tremendously increased with the drastic changes in information technologies. These cyber-attacks are becoming increasing complex. Many software systems quality attributes at the moment have security topping the list. Cyber-attacks and other cyber threats can cause disastrous impacts in a community, especially for a coordinated attack targeting multiple critical infrastructures. This crime is often rampart on Web-based systems that are accessible online via the Internet. Some institutions in fear of this attack have chosen to shelve online processing to more secure intranets that only allow accesses on their local area networks. (Romero-Mariona et. al, 2009).

### 2.4.2 Some of the attack tools likely to be used:

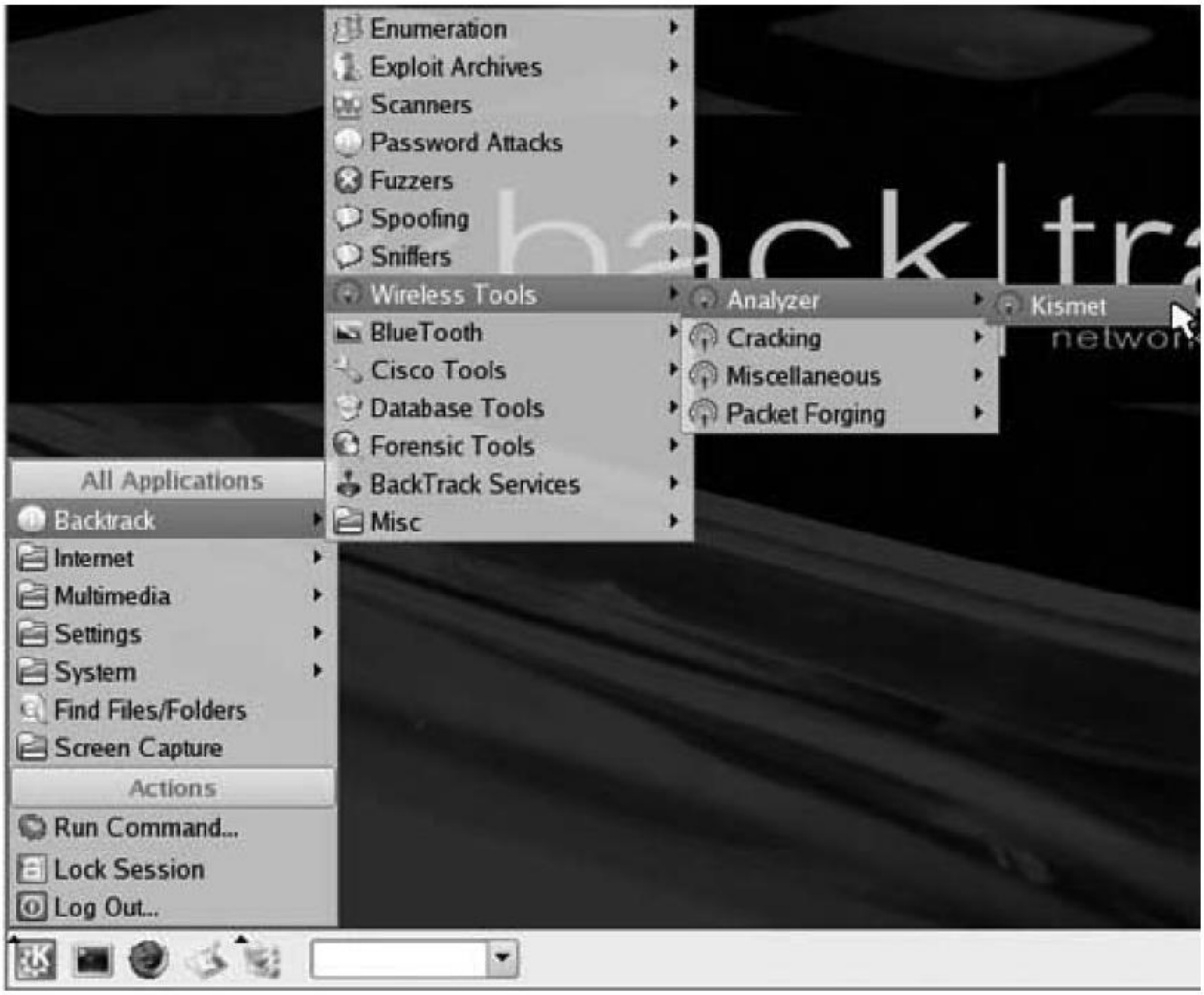



**Figure 1-2** Menu of attack tools

The Internet structure lacks a single central control **(**Peisert et. al, 2014). Therefore, anyone connected online can carry out legitimate or malicious tasks. Cybercrimes exploit this unstructured nature of the Internet. In addition, individuals with expertise on programming and other complicated computing skills are the majority involved in compromising the security of the computer users. Currently, there are many online tools that are misused. Software developers who contravene software engineers' professional code of ethics can be cited as the source of cyber-attacks. The primary target of most reported cybercrimes in Kenya in (2014) targeted key government institutions' websites. Successful cyber-attacks in Kenya are blamed on poor detection tools and a lack of capacity to address the crime. (Summerville, 2011).

### 2.4.3 Type of attacks likely to affect most of the learning institutions:

**Viruses and worms** - Viruses and worms are computer programs that affect the storage devices of a computer or network, which then replicate information without the knowledge of the user

**Spam emails** - Spam emails are unsolicited emails or junk newsgroup postings. Spam emails are sent without the consent of the receiver potentially creating a wide range of problems if they are not filtered appropriately.

**Trojan** - A Trojan is a program that appears legitimate. However, once run, it moves on to locate password information or makes the system more vulnerable to future entry. Or a Trojan may simply destroy programs or data on the hard disk.

**Denial-of-service** - DoS occurs when criminals attempt to bring down or cripple individual websites, computers or networks, often by flooding them with messages.

**Malware** - Malware is software that takes control of any individual's computer to spread a bug to other people's devices or social networking profiles. Such software can also be used to create a 'botnet' a network of computers controlled remotely by hackers, known as 'herders,' to spread spam or viruses. Scareware Using fear tactics, some cyber criminals compel users to download certain software. While such software is usually presented as antivirus software, after some time these programs start attacking the user's system. The user then has to pay the criminals to remove such viruses.

**Phishing** - Phishing attacks are designed to steal a person's login and password. For instance, the phisher can access the victims' bank accounts or assume control of their social network.

**Fiscal fraud** - By targeting official online payment channels, cyber attackers can hamper processes such as tax collection or make fraudulent claims for benefits.

N/B: (Monitor, July 2011).

## 2.5 Prevalence of Cybercrime Activities against the Learning Institutions In Terms Of Degree, Level, and Distribution.

Most of the Kenyan learning institutions have seriously become prevalent to the latest cybercrime trends. A lot of cases on complications such; Network systems complications, Password cracking, Problems with Newly implemented systems e.g. ERP, Data loss, problems associated with the E-learning programmes.

### 2.5.1 Network systems complications.

Most of the institutions networks are insecure thus giving loophole for malicious activities. Such activities are carried by malicious individuals within the institution. They may include:

### 2.5.2 Hacking of the institutional Network.

In serious cyber security trends in most institutions this grabs high percentage as most of the individual within the institutions tend to malicious in consolidating their gains i.e. testing their ability on how strong they are to cause threat to the entire network, testing their skills on hacking processes.

Most of the students are categorized as script kiddies they mainly depend on downloaded scripts on hacking strategies and they are curious on testing how effective they are. Upon carrying out the test, they end up causing great problem to the entire institutional network.

This shows how serious the crime is and the main targets for the practice of the skills are the learning institutions before an extension to the outside world.

### 2.5.3 How Attackers Evade Network Security.

They Hide during Network Delivery using advanced evasion techniques (AETs); crafty attackers avoid network detection by breaking up file (malware) packets into hard-to-inspect patterns.

They Go Dormant during Analysis- to evade sandboxes closed security environments that closely analyze the behavior of a suspect file malicious file know when they’re in one, and remain silent.

They stay Covert during Callback Once on the endpoint, sophisticated malware avoids abnormal behavior or uses randomized callback connections to evade security devices and continue malicious activity.

### 2.5.4 Downtime to network users within the institutions.

This normally experienced in most institutions as a result of the flooding of the network that is caused by: flooding of the server with several requests, high number of network users that cannot be supported with the available bandwidth over the internet. This has been a serious case in the University of Jaramogi Oginga Odinnga of Science and Technology as a result of the creation of rogue networks by the students that leads high use of the bandwidth hence eventually leading to disruption in most sectors within the university.

### 2.5.5 Total Network failure in the institutions.

This normally conducted either online by malicious individuals within the network or outside the network. Such malicious individuals may pose certain threats that when fully exploited leads total network failure.

Most of vandalism cases have been observed in most of the institutions the destruction of the Wi-Fi access points in the institutions, cutting off of the Ethernet cables i.e. JOOUST, this has led to network failures in the university.

### 2.5.6 Data loss.

Data loss is any process or event that results in data being corrupted, deleted and or made unreadable by a user or software or application. Data loss can occur on any device that stores data. Even a simple misplacement of data, is by definition technically a loss. This calling for Data loss prevention (DLP) which is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. (Disclosure, 2008).

Data loss may occur in the following categories:

#### 2.5.6.1 Information Leakage.

Information leakage (also known as data leakage) is when sensitive data are revealed intentionally or not intentionally to unauthorized parties. The information leaked out can either be private in nature and are deemed confidential, such as credit card numbers or information that could be used by attackers to further exploit the system, (Information Leakage, 2005).

Origination of Information Leakage can occur in the common ways corporations envision. Many organizations may invest heavily into firewalls, anti-virus software, encryptions and intrusion detection systems in order to protect loss of data to unauthorized parties such as external hackers

Data leakages can also occur through comments left by a developer in the system script codes or HTML for future debugging or integration, providing unauthorized parties view of how scripts work or even passwords and usernames used during the development phase (Mallery, 2009).

It appears that data leakage occurs mostly from insiders of the organization. This is supported by one of study which found that, 87% of confidential information leaked out is from insiders Therefore, this is important for the management to take note of. (Baek, Kim, & Lee, 2008).

**2.5.6.2 Impact of Data Leakage.**

The impact of data leakage to an organization can become severe and costly; therefore this issue is extremely relevant for management to consider. Although at first, organizations may not notice any immediate effects, the "small bits and bytes leaving the organization day by day" can result in considerable business costs that are difficult to quantify (Zinkewicz, 2009). According to a research conducted by US security think tank, Ponemon Institute, through interviewing 56 US companies, the average leak per company was valued at more than AU$6 million Average Cost of Data Leak, (2006). Not only is this an impact on a company's bottom line, a corporation's brand value can also be eroded (as customer and shareholders lose faith in the corporation's controls), taking years to recover. With companies holding increasing amounts of privacy data now, such as social insurance numbers of employees or credit card information of customers, the leakage of data can allow unauthorized parties to use it for criminal activities like identity theft. As such, in the US, legislations have been enacted. For more than 40 states, companies are now required to notify customers if their information was compromised (Zinkewicz, 2009).

Furthermore, data leakage can also wreak havoc for institutions plans and deals. According to a study performed by Cass, commissioned by an online workspace provider, Intralinks looked at more than 350,000 transactions between 1994 and 2007 that were leaked ahead of time and found that more than 50% did not run to completion or on average, took longer to complete (MacFadyen, 2008). Thus, dealmakers will have to work harder to complete the deals as the leak (to the press) may have changed the context of the negotiations (MacFadyen, 2008).

## 2.6 Problems associated with E-Learning.

Most universities are in the race of formulating e-learning. The implementation is basically relied on the use internet as the main platform for effective performance of the enacted programme. However they try to automate most of the learning activities in line with the Kenyan vision 2030, the implementation is succumbed with various issues that lower its functionality where as the key issue being the cyber-security in most of the Kenyan learning institutions.

The programme is mainly supported on internet basis that is full of cyber security threats that hinder proper utilization of the implementation. Such cyber security trends may include:

**2.6.1 Information theft** for illegal business like plagiary-malicious individuals may gain unauthorized access to key information on a given site of on a given site of e-learning to satisfy their needs.

**2.6.2 Deletion and alteration of information-** certain information may be deleted or altered by unknown individuals that might be a big blow to the beneficiaries of the programme.

### 2.6.3 Cyber stalking.

Cyber stalking is the use of technology to harass someone. An attacker harasses a victim using electronic communication, such as e-mail, instant messaging (IM), phone calls or posting messages on chat forums discussion groups or social sites. A cyber stalker will hide in the Internet for anonymity to avoid detection. The stalker relies upon the anonymity afforded by the Internet to allow them to stalk their victim without being detected. In Kenya cyber stalking takes many forms such as defamation or libel, falsification, fraud, intimidation, offensive comments, personal attacks, graphic violence and violation of rights to privacy. Cyber stalkers will go to great lengths to try to monitor a victim's online activity. This may include infecting a person's computer with malware that is able to log computer activity. Most learning institutions with the automation programme are likely to face challenges associated with the cyber stalking. Stalkers are capable of making access to some confidential information of the institution or even likely to cause disruption to the users. (International Journal of Education and Research Vol. 3 No. 11 November, 2015).

### 2.6.4 Malware attack.

Malware refers to malicious software that finds their way to a computer system especially from the Internet. They could be viruses, Trojans worms, and other software that get installed in a computer without the user's knowledge. In several cases, the software will pretend to be legitimate software. Malware's intentions are diverse ranging from spying on your work, phishing of password or password sniffing, monitoring web sites visited access to confidential data, and denial of service, among others. Since the e-programme being an internet aided it is likely to face most of the Trojan attacks. (International Journal of Education and Research Vol. 3 No. 11 November 2015).

### 2.6.5 Identity theft or Fraud.

Most of the learning institutions are prone to identity theft or fraud whereas Cybercriminals obtain personal and confidential data belonging to someone or an institution they are targeting. This information can be obtained through social engineering, email phishing, purchase the data on the black market, or use tools and techniques to search. A majority of personal data is the open access in the Internet especially in this era of socializing sites. An attacker may befriend a non-suspecting individual and obtain all the information they needed to launch an attack or entice them to perform some action. This likely to cause fear on most of the system users who are likely to be students, staff-members. (International Journal of Education and Research Vol. 3 No. 11 November 2015).

### 2.6.6 Spamming attack.

Spamming involves flooding the internet with many copies of the same message to multiple addresses. A spammer sends millions of emails in hope that one or two percent will find their way into inboxes and that a further one or two percent will generate a response. Spam messages are always sent with false return address information and they are also referred to as junk mail (Milhorn, 2007).

The table is giving illustrations on various forms of cyberspace crimes. The table is viewed in terms of research analysis done where the respondents were asked to indicate the forms of cybercrime prevalent in Kenya, on a five likert-scale where Very Great Extent = 5; Great Extent = 4; Average extent = 3; Small Extent = 2; Very Small Extent = 1.

| **Forms of Cyberspace crime** | **Mean** | **Percentage (%)** |
|---|---|---|
| Spam | 4.70 | 94 |
| Viruses & Trojans | 4.43 | 88 |
| Hacking | 4.27 | 85 |
| Piracy | 4.10 | 82 |
| Phishing | 3.87 | 77 |
| Denial of service | 2.60 | 52 |
| Cyber espionage | 1.47 | 29 |
| Cyber stalking | 1.20 | 24 |
| Cyber terrorism | 1.07 | 21 |
| Cyber pornography | 3.13 | 62 |

**Table2.0 Forms of Cyberspace crimes.**

From the results in table 2.0, it was found that, Spam, virus and Trojan attacks, hacking and piracy, were the leading cyberspace crimes experienced.

Other cyberspace crimes that are emerging include; Cyber espionage, Denial of Service attacks, Cyber terrorism and Cyber stalking. These can be explained to be at the bottom of the table largely as a result of the fact that, internet in Kenya is still developing where internet is still expensive and limited but once the fiber connectivity is fully operational these threats are feared to be escalated, since internet will be readily available at cheaper rates and bandwidth connectivity will compare to first world economies. Cyber terrorism the most feared of them all poses a great danger especially as the government plans to inter-connect all its ministries through e-governance (great threat to Kenyan vision 2030). It faces a deadly threat where its operations may be interrupted through denial of service attacks that could cripple vital services. Again, cyber espionage may be used to steal or expose critical information by covert organizations intending to sabotage the state. (CID, January 2005).

### 2.6.7 System Hacking.

Most of the students mainly target the institutions system in order to make alterations i.e. they majorly seek unauthorized penetration to the database for grades alterations, change of fee balances, and even posing threats to the entire system of total failure. A report has been issued showing that most of the university students are regarded as the most malicious hackers. Out curiosity most of the students have tried their best to pose danger to the administration's systems by hacking the system to ensure a total failure. Institutions of higher learning in Kenya are now feeling the heat of cybercrime as students target their databases. (Cyberoam report, 2016).

# CHAPTER 3.

## 3.0THE STUDY METHODOLOGY

### Mixed Methods Research Methodology

The study adopted mixed methods research methodology. Mixed methods research is a methodology for conducting research that involves collecting, analyzing, and integrating or mixing quantitative and qualitative research and data in a single study. The purpose of this form of research is that both qualitative and quantitative researches, in combination, provide a better understanding of a research problem or issue than either research approach alone (Teddlie,2003).

This approach focuses on collecting both quantitative and qualitative data and mixing the data. It also involved integrating quantitative and qualitative approaches to generating new knowledge and can involve either concurrent or sequential use of these two classes.

According to Dr. Bulsara, she mentioned some of the key qualification factors for the use of mixed methods research methodology for a given study:

Variation in data collection leads to greater validity.

Answers the question from a number of perspectives.

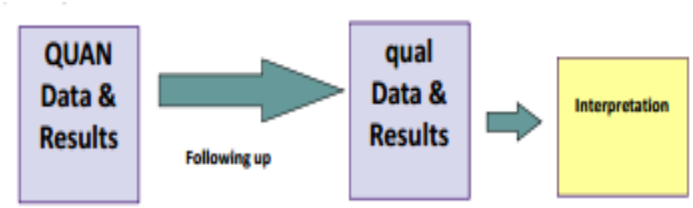
Ensures that there are no ‘gaps’ to the information or data collected.

Ensures that preexisting assumptions from the researcher are less likely.

When one methodology does not provide all the information required

The study picked on the Sequential Mixed Methods Design that calls for the analysis of both the qualitative and quantitative data collected then merging the two for interpretations.

Sequential Mixed Methods Design



Quantitative research questions will address the research question or issue. Information from the first phase will be explored further in a second qualitative phase whereas qualitative data collection will be used to explore important quantitative results. The reason for following up with qualitative research in the second phase is to better understand and explains the quantitative results.

The concepts of the strategic studies on security will be discussed in details in order to convey the meaning and understanding of the security in the current century. The study is focused on the latest cybercrime trends in Kenyan learning institutions. It will address the effects of such crimes and their dangers to Kenyan plan on vision 2030.

### 3.1.1 Data Collection Procedures and Instruments:

The instruments used to obtain data in this research are:

**3.1.1.1 Primary sources** – primary sources are regarded as the first handed information such as official government strategies and document pertaining to cybercrime and cyber security and observations.

**3.1.1.2 Secondary sources** - secondary source includes books, journal articles, among others.

**3.1.1.3 Survey** - using structured questionnaires. Looking forward for more information, this involved the interviewing of some of the university students to get more information on the area of study with the aid of open ended questions and closed ended questions.

**3.1.2 Target group** – The study focused on a huge population in a certain university of science and technology whereas main interest was to get ideas from some of them thus settling on a portion of the population of twenty students only. This was due to time schedule of the study that limited interaction with other individuals for more information hence limiting to a few number as twenty students only within learning institution of Jaramogi Oginga Odinga University of Science and Technology.

### 3.1.3 Target areas

This study had a plan of extensive exploration in institutions such as universities, colleges and high schools for data collection, a sample of learning institution of science and technology has been used to meet the goals of the set objectives.

### 3.1.4 Study design

This research has included real life stories identified through reports, observations on the research areas.

### 3.1.5 Research Structure

The research will contain five chapters in which:

**Chapter 1**. Serves as the introduction in order to clarify the scope and focus of the research.

**Chapter 2**. Majorly dwells on literature review, conceptual frame work on the cybercrime trends, how prevalent Kenyan learning institutions have become to cybercrime.

**Chapter 3.** Dwells on the research methodology and the structure of the study.

**Chapter 4.** This chapter is based on the study on cybercrime in Kenyan learning institutions thus shows:

Rapid growth of internet use in Kenya, internet supported programmes within the learning institutions, role of government in support to the internet users, cybercrime trends as an emerging threat to Kenyan learning institutions.

**Chapter 5.** Kenya response to the latest cybercrime trends in the learning institutions. This includes the findings from questionnaires that gives conclusion of the matter, summary and recommendations after thorough analysis of data.

### 3.1.6 Data Analysis method

All the respondents responses were plotted in a likert-scale with various values that were used in excel to generate the average, percentage values, and the bar graph after all the analysis.

### 3.1.7 Descriptive statistical method, a 5-likert-scale and Microsoft excel.

In this research the descriptive statistical method is applied with the use of five-likert scale.

According to Saul McLeod he mentioned that likert scale majorly implies the measuring of attitude by asking people to respond to a series of statement about a topic in terms of the extent to which they agree with them and so tapping into the cognitive and effective components of attitudes.

The likert-scale fixed choice response format and are designed to measure attitudes or opinions. This ordinal measure levels of agreements or disagreement. (Burns and Grove 1997).

A likert type scale assumes that the strength or intensity of experience is linear that is on a continuum from strongly agree to strongly disagree and makes the assumption that attitudes can be measured. Respondents may be offered a choice of five to seven or nine pre-coded responses with the neutral point being neither agree nor disagree. (Bowling, 1997).

### 3.1.8 How to analyze Data from a likert-scale

Summarize using a median or mode; the mode is probably the most suitable for easy interpretation. Display the distribution of observations on a bar chart. (Bowling, 1997).

### 3.1.9 Why likert-scale is used as a method of data analysis

They have the advantage that they do not expect a simple Yes or No answer from the respondents, but rather allow for degrees of opinion and even no opinion at all. Therefore quantitative data is obtained which means that the data can be analyzed with relative ease. (Bowling 1997).

The validity of likert scale attitude measurement can be compromised due to social desirability. This implies that the individual may like to put themselves in a positive light. (Bowling, 1997).

### 3.1.10 Steps on making Likert-scale

1. Define what is measured- it is unidimensional scaling method, it is assumed the concept you want measure is one dimensional in nature.
2. Set (create the set of potential scale items). They should be rated on a one to five or one to seven, disagree – agree response scale.
3. Rating the items – have a group of judges rate the items. Usually you would use one to five rating scale.
    - Strongly and favourable to concept
    - Somewhat unfavourable to the concept

- Undecided
- Somewhat favourable to the concept
- Strongly favourable to the concept

4. Selecting items – this involves computing intercorrelations between all pairs of items based on the rating of judges on what item to retain for final scale.
5. Admistering the scale – use rate of one to five.
    - Strongly disagree = 1
    - Disagree = 2
    - Neutral = 3
    - Agree = 4
    - Strongly agree =5

Using ordinal data it shows the difference between the scores but it cannot state the exact value which is shown by the interval data.

Adding a response of strongly agree to other two responses calls for getting the mean. The best method to use is the use of mode.

N/B: This method of data analysis does not allow the mention of the audience for the presentation.

## 3.2 The sampling frame of the study

### 3.2.1 Simple Random sampling

Sampling refers to a small part or quantity intended to show what the whole is like.

Simple sampling (random sampling)

Is a subject of individual (a sample) chosen from a largest set (a population). Each individual is chosen randomly and entirely by chance such that each individual has the same probability of being chosen at any stage during the sampling process, and each subset of k individuals has the same probability of being chosen for the sample as any other subset of k individuals this refers to simple random sampling.

**Why random sampling has been used in this research**

It is an unbiased survey technique.

Principle  simple random sampling is that every object has the same probability of being chosen.

**Advantages of simple random sampling**

It is free of classification error

Requires minimum advanced knowledge of the population other than the frame.

It is relatively ease to interpret data collected in this manner.

# CHAPTER 4.

## 4.0 STUDIES ON CYBERCRIME TRENDS IN KENYA.

### 4.1 Introduction.

Cybercrime has become a global concern, particularly in rapidly developing countries like Kenya. Kenya's ICT revolution followed the laying of undersea cables in 2009. Kenya's growth in Internet use has been facilitated by high proliferation and adoption of mobile communications. Speedy diffusion and adoption has exposed the Kenyan public to unprecedented individual security threats. A national drive to foster awareness and nurture detection and coping skills is urgently required

### 4.1.1 Rapid growth of internet use in Kenya.

Development of the Internet in Kenya took place in three broad phases. The first phase, which ran from 1990 to 1998, witnessed the introduction of the Internet largely by Kenyans returning from studies overseas, western expatriates, and personnel of Inter-governmental Organizations and NGOs. Commercial ISPs entered the Internet market by the mid-1990s, primarily offering dial up and content services. The early adopters of the Internet included import or export sector, industries with overseas clients and the academic sector. Most of the Internet users then were confined to the Capital City, Nairobi. As the number of ISPs and Internet users increased, the need for an Internet backbone became evident and the defunct Kenya Posts and Telecommunications Corporation established one in 1998. The key challenges in the 1990s included limited and high cost of international Internet bandwidth; the high cost of both dial-up and domestic leased lines; the limited penetration of PCs; lack of policy and regulatory environment; and the lack of appropriate IT skills (Njoroge, 2009).

The second phase took place from 1999 to 2004 with the Government of Kenya restructuring the communications sector with a view to introducing competition and to pave way for private sector participation. As a result, an independent ICT sector regulator, the Communications Commission of Kenya (CCK), was established to spearhead sector reform. A number of positive developments took place during this phase; the most notable were the establishment of an Internet Exchange Point (IXP) by the private sector and the successful re- delegation of the administration of dot KE TLD through a public private partnership. The elapse of Telkom Kenya's exclusivity in June 2004 in the provision of various services including Internet

bandwidth marked the grand entry of the third phase of Internet development in Kenya. At this moment, the most serious threat to the economy is seen as the lack of security online. (Cyber security, 2011).

According to the latest usage report from communication authority of Kenya, there were an estimated 26.1 million internet users in Kenya as of December 2014. This represents 64% of the entire population with access to the internet and over 70% being below 25 years. (Serianu, 2015).

### 4.1.2 Cybercrime – a growing challenge for government.

In a digital age, where online communication has become the norm, internet users and governments face increased risks of becoming the targets of cyber-attacks. As cyber criminals continue to develop and advance their techniques, they are also shifting their targets — focusing less on theft of financial information and more on business espionage and accessing government information. Advancements in modern technology have helped countries develop and expand their communication networks, enabling faster and easier networking and information exchange. Currently, there are nearly 2 billion internet users (Monitor, 2011).

The growing popularity and convenience of digital networks, however, come at a cost. As businesses and societies in general increasingly rely on computers and internet-based networking, cyber-crime and digital attack incidents have increased around the world. These attacks generally classified as any crime that involves the use of a computer network include financial scams, computer hacking, downloading pornographic images from the internet, virus attacks, e-mail stalking. (Monitor, 2011).

### 4.1.3 Increasing cybercrime.

Over the past few years, the global cybercrime landscape has changed dramatically, with criminals employing more sophisticated technology and greater knowledge of cyber security. Until recently, malware, spam emails, hacking into corporate sites and other attacks of this nature were mostly the work of computer ‘geniuses’ showcasing their talent. These attacks, which were rarely malicious, have gradually evolved into cybercrime syndicates siphoning off money through illegal cyber channels. By 2010, however, politically motivated cybercrime had penetrated global cyberspace. In fact, weaponry and command and control systems have also transitioned into the cyberspace to deploy and execute espionage and sabotage, as seen in the

example of digital espionage attacks on computer networks. (Cyber Crime – A Growing Challenge for Governments, 2011).

Various analyses that have been done on this have shown that: In 2010, the global spam rate increased from 1.4 percent year-on-year, to 89.1 percent, most of which involved botnets, (Symantec report, 2011).

In 2010, the average rate of malware in e-mail traffic was 1 in 284.2 e-mails, almost the same as that in 2009. However, the average rate of e-mails blocked as phishing attacks improved from 1 in 325.2 in 2009 to 1 in 444.5 in 2010. (Symantec report 2011).

The average number of blocked malicious websites rose from 2,465 per day in 2009 to 3,188 in 2010. (Symantec report 2011).

In 2010, a major attack came from a complicated computer worm Stuxnet. The worm which infected a large number of industrial controls worldwide was able to give false machinery instructions, subsequently leading to nuclear malfunctions and break-down operations. (Symantec report, 2011).

Cyber criminals are now moving beyond computers, and attacking mobile handheld devices, such as smartphones and tablet personal computers (PCs). (Symantec report, 2011).

### 4.1.4 The Concept of Cybercrime.

It is stated that concept of cybercrime is not so much different from that of conventional crime as both include conduct, whether act or omission, which cause breach of rules of law and counterbalanced by the sanction of the state. Current definitions of Cybercrime have evolved experientially and differ depending on the perception of both observer or protector and victim. (Zeviar-Geese 1998).

When speaking about cybercrime, usually it is about two major categories of offences. In one, a computer connected to a network is the target of the offence and this is the case of any crime that is facilitated or committed using a computer, network, or hardware device. The computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime. The crime can take place on the computer alone, or in other non-virtual locations. (Taylor, 1999).

### 4.1.5 Common cybercrime activities:

**Unauthorized access of hosts** more commonly known as hacking, can take various forms some of which might not always involve deep technical knowledge. It involves using a computer or terminals to crack the security of some computer systems. Cybercriminals use snifters or just by guessing passwords to breach security greatly diminishing the effectiveness of passwords when users do not select wisely (Adomi, 2008).

**Spamming** involves flooding the internet with many copies of the same message to multiple addresses. A spammer sends millions of emails in hope that one or two percent will find their way into inboxes and that a further one or two percent will generate a response. Spam messages are always sent with false return address information and they are also referred to as junk mail (Milhorn, 2007).

**Viruses, Trojans and Worms** all fall into a similar category as they are software designed to infect computers or install themselves onto a computer without the infrastructure to generate mass fear and anxiety (Wall, 2007).

**Cyber terrorism** is the convergence of terrorism and cyberspace. It has been defined as premeditated, politically, motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub national groups or clandestine agents. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact (Khosrowpour, 2004).

All stages of computer operations are susceptible to criminal activity, either as the target of fraud, the instrument of fraud, or both. Input operations, data processing, output operations and communications have all been utilized for illicit purposes. (Siegel, Saukko, & Knupfer, 2000).

### 4.2 Motivations of cybercrime in most organisations:

There are a number of general motivations for cybercriminals to continue in their endeavors:

Lack of legislation touching on cyber-attacks.

Poor detection techniques. Mechanisms of tracking the culprit are much behind.

Lack of capacity to respond to the crime. This exposes vulnerability of systems in Kenya. Attackers are also capitalizing on the naivety of some of the Internet system users. Numerous "mouse click events" without thought of what is likely to happen next. (International Journal of Education and Research Vol. 3 11 November 2015).

### 4.3 Challenges in Curbing Cybercrime.

There are a number of strategies employed by various organizations some specific to particular cybercrime forms and some general for instance, antispam which is specific to preventing the proliferation of spam mails into client accounts which is also a part of CCK requirement to ensure that clients are protected.

General strategies against cybercrime include use of firewalls and bandwidth shaping tools, for instance, the Canadian developed Sandvine equipment which limits bandwidth choking and efficient way of controlling piracy.

It is hard to convict cyber criminals because of two major reasons. Firstly, few countries have enacted e-laws and the existing ones are not sufficient in convicting culprits because of jurisdiction anomalies especially when the investigation transcends international borders. Secondly, obtaining evidence of computer crime that would stand in courts of law is lacking in many countries since the field of computer forensics is still relatively new and lacks sufficient literature and expertise. (Cyber security, 2011).

#### 4.3.1 Reliance on ICTs.

It has been mentioned that many everyday communications depend on ICTs and Internet-based services, including VoIP calls or e- mail communications. ICTs are now responsible for the control and management functions in buildings, cars and aviation services. The supply of energy, water and communication services depend on ICTs. The further integration of ICTs into everyday life is likely to continue. Growing reliance on ICTs makes systems and services more vulnerable to attacks against critical infrastructures. Even short interruptions to services could cause huge financial damages to e-commerce businesses. It is not only civil communications that could be interrupted by attacks; the dependence on ICTs is a major risk for military communications. (Understanding cybercrime, 2012).

Existing technical infrastructure has a number of weaknesses, such as the monoculture or homogeneity of operating systems. Many private users and SMEs use Microsoft's operating system, so offenders can design effective attacks by concentrating on this single target. (Understanding cybercrime, 2012).

### 4.3.2 Number of users.

The popularity of the Internet and its services is growing fast, with over 2 billion Internet users worldwide by 2010. Computer companies and ISPs are focusing on developing countries with the greatest potential for further growth. In 2005, the number of Internet users in developing countries surpassed the number in industrial nations, while the development of cheap hardware and wireless access will enable even more people to access the Internet. With the growing number of people connected to the Internet, the number of targets and offenders increases. It is difficult to estimate how many people use the Internet for illegal activities. Even if only 0.1 per cent of users committed crimes, the total number of offenders would be more than one million. Although Internet usage rates are lower in developing countries, promoting cyber security is not easier, as offenders can commit offences from around the world. The increasing number of Internet users causes difficulties for the law-enforcement agencies because it is relatively difficult to automate investigation processes. (Understanding cybercrime, 2012).

# CHAPTER 5:

## 5.0 RESEARCH FINDINGS AND ANALYSIS.

### 5.1 Research Strategy.

The guiding principles here were the objectives of the study. A survey research design sought information about the effects of Cybercrime on Kenyan learning institution. This study had the privilege of providing in-depth analysis on the recent internet development in Kenya and the challenges it imposes on state security.

The population of the study consisted of twenty students of the Jaramogi Oginga Odinga university of Science and Technology in different faculties with main focus on the ones taking computer related courses. The frame sample constitutes of both the students in IT related courses and even the ones taking non IT related courses where simple random sampling was employed to select the respondents in this study. With Simple Random Sampling, a random sample was selected such that every element in the population supposed to have an equal chance of being included into the sample and the respondents selected.

The mechanisms employed in data collection included the use of both questionnaires and interviews (See appendix1). The questionnaires were preferred in this study because those who took part in this study were considered to be literate and capable of answering the questions sufficiently. With the help of Microsoft excel was used to analyze data thus giving guidelines in the plotting of the required bar-graphs per the statistical analysis.

### 5.2 Data Analysis and Findings.

Data was collected from twenty (20) students with only fifteen (15) of them responding. All the students interviewed consented to their knowledge and existence of Cybercrime in Kenya learning institutions.

#### 5.2.1 Forms of Cybercrime Prevalent In Kenya.

There are a number of forms of cybercrime. The respondents were asked to indicate the forms of cybercrime prevalent in Kenyan learning institutions, on a five likert-scale where Very Great Extent = 5; Great Extent = 4; Average extent = 3; Small Extent = 2; Very Small Extent = 1. The results are shown on table 5.0

**Table 5.0 Forms of cybercrime in the institutions.**

| Forms of cybercrime | Mean | Percentage (%) |
|---|---|---|
| **i. Spam mail** | 4.7 | 94 |
| **ii. Denial of service** | 2.6 | 52 |
| **iii. Cyber stalking** | 1.2 | 24 |
| **iv. Hacking** | 4.2 | 85 |
| **v. Cyber Espionage** | 1.4 | 29 |
| **vi. Phishing** | 3.8 | 77 |
| **vii. Others specify** | - | - |

From the table 5.0 it was found that, Spam mails, hacking and phishing attacks, are the leading cybercrime experienced by learning institutions. Most of the attacks seam unreported. Otherwise most victims preferred to keep quiet because they do not think reporting would help them since preserving evidence is unknown to them. These statistics relates to a reported that states, Kenyans and internet users are initiating and falling victim of cybercrime, although the public are not reporting to the relevant authorities either because of non-existent sensitization programs or hopelessness due to the unavailability of e-laws that would bring them justice.

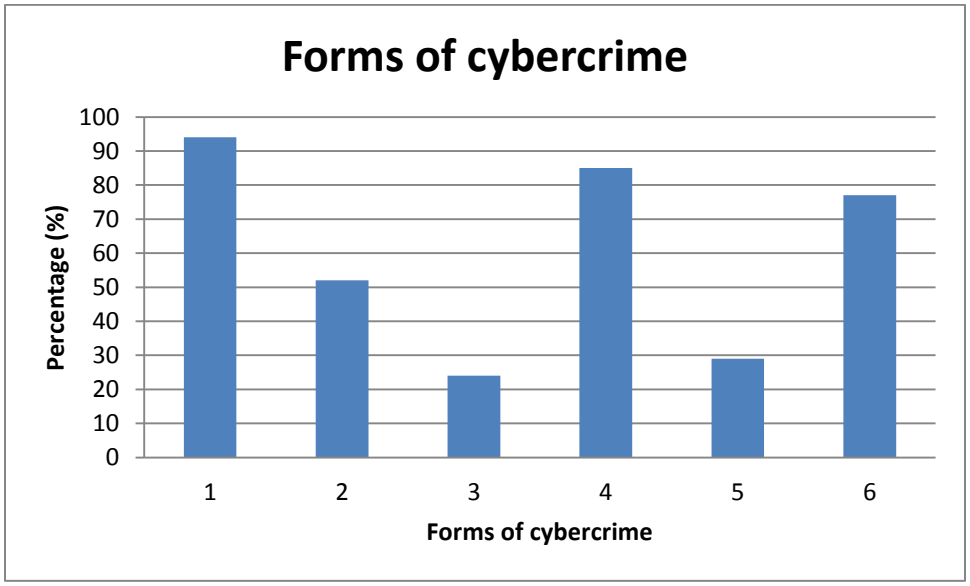


**Fig 5.0 showing the forms of cybercrimes in the learning institutions**

| Key: | % |
|---|---|
| **1. Spam mail** | 94 |
| **2. Denial of service** | 52 |
| **3. Cyber stalking** | 24 |
| **4. Hacking** | 85 |
| **5. Cyber Espionage** | 29 |
| **6. Phishing** | 77 |

### 5.2.2 Challenges on Curbing Cybercrime.

There are a number of strategies employed by various institutions some specific to particular cybercrime forms and some general for instance, antispam which is specific to preventing the proliferation of spam mails.

The respondents, therefore, were queried on a number of challenges they are facing in fighting cybercrime in the learning institutions. This was on a five likert-scale where Very Great Extent = 5; Great Extent = 4; neither agree nor Disagree = 3; Small Extent = 2; Very Small Extent = 1 where the higher values represented the extent to which the challenges had been overcome, on the other hand, the lower values represented the challenges that were still difficult to eliminate. The results are shown on the table 5.1

**Table 5.1 Challenges on Curbing Cybercrime.**

| Challenges | Mean | Percentage (%) |
|---|---|---|
| **i. Software evaluation** | 2.1 | 42 |
| **ii. Management training** | 3.4 | 68 |
| **iii. Compatibility issues** | 4.4 | 88 |
| **iv. Resistance to change** | 3.9 | 78 |
| **v. Skilled personnel** | 1.9 | 38 |
| **vi. Adequate staff** | 1.9 | 38 |

| | | | |
|---|---|---|---|
| **vii.** | **Cost** | 3.7 | 74 |
| **viii.** | **Cybercrime awareness** | 3.1 | 62 |
| **ix.** | **ignorance** | 3.8 | 76 |

From table 5.1, it was found that most learning institutions have got serious issues when it comes to cybercrime control the compatibility issues takes the highest percentage whereas most of the techniques used are not user compatible. Though greater number is aware of the cybercrime activities but still there is a great challenge when it comes to control as most of the learning institutions have low percentage of skilled personnel to help in controlling most of the cybercrime activities. The state of ignorance in most of the institutions is alarming thus leading to poor mechanisms in controlling most of the cybercrime activities from affecting most of the learning institutions. It is true that the institutions managers are pushing for change but it has been too hard as greater percentage 74% is resistance to change.

Bar-graph showing challenges on curbing cybercrime in the learning institutions.

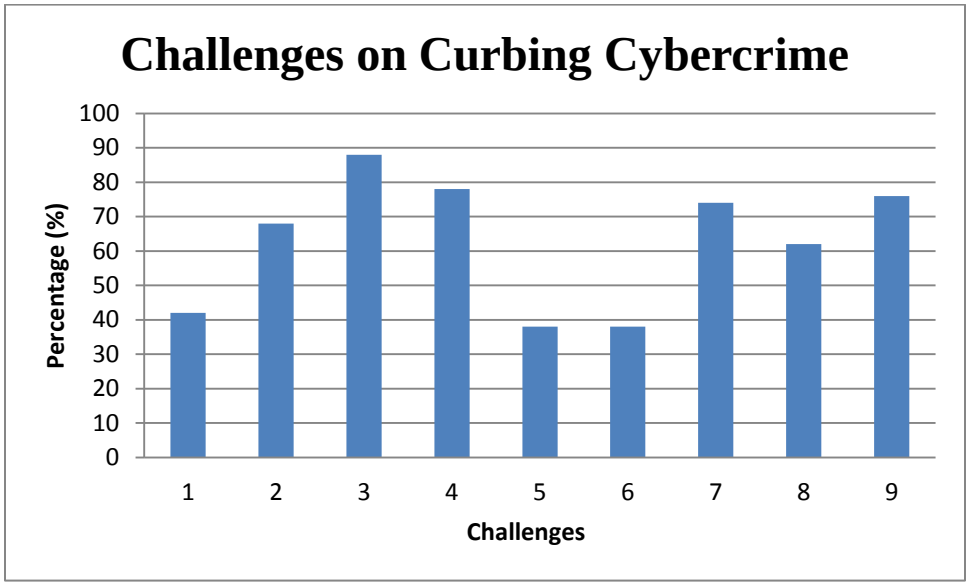


**Fig 5.1 showing challenges on curbing cybercrime in the learning institutions in Kenya.**

| key | % |
|---|---|
| **1. Software evaluation** | 42 |
| **2. Management training** | 68 |
| **3. Compatibility issues** | 88 |
| **4. Resistance to change** | 78 |
| **5. Skilled personnel** | 38 |
| **6. Adequate staff** | 38 |
| **7. Cost** | 74 |
| **8. Cybercrime awareness** | 62 |
| **9. ignorance** | 76 |

### 5.2.3 Preventing Cybercrime.

The respondents were asked to identify the various strategies they had employed in order to curb cybercrime. This was on a five likert-scale where Very Great Extent = 5; Great Extent = 4; Average extent = 3; Small Extent = 2; Very Small Extent = 1. The responses are as shown on the table 5.2.

**Table 5.2 Preventive measures on Cybercrime.**

| Measures | Mean | Percentage (%) |
|---|---|---|
| **1. Antivirus** | 4.7 | 94 |
| **2. Software firewall** | 4.3 | 86 |
| **3. Antispam blocker** | 4.6 | 92 |
| **4. Data encryption** | 3.8 | 76 |
| **5. Data recovery strategies** | 3.8 | 76 |
| **6. Staff training awareness on cybercrime** | 4.3 | 86 |
| **7. Penetration testing** | 2.6 | 52 |
| **8. Bandwidth management** | 3.2 | 64 |
| **9. Hardware firewall** | 1.2 | 24 |
| **10. Customer behavior policies on cybercrime** | 2.6 | 52 |
| **11. Parental control software** | 2.6 | 52 |

From the results in table 5.2, it was found that a great extent (mean>3) the management committee have focused on employing antivirus applications, software firewalls, antispam applications, data recovery and staff training in an effort to control cybercrime in the institutions. Although there is an indication that the management personnel have tried to focus on ways of preventing cybercrime, other important areas such as parental control which can be an effective measure against cyberpornography and also penetration testing to identify loop holes that can be exploited by cybercriminals, haven't yet been fully looked into.

Bar-graph showing measures on preventing cybercrime.

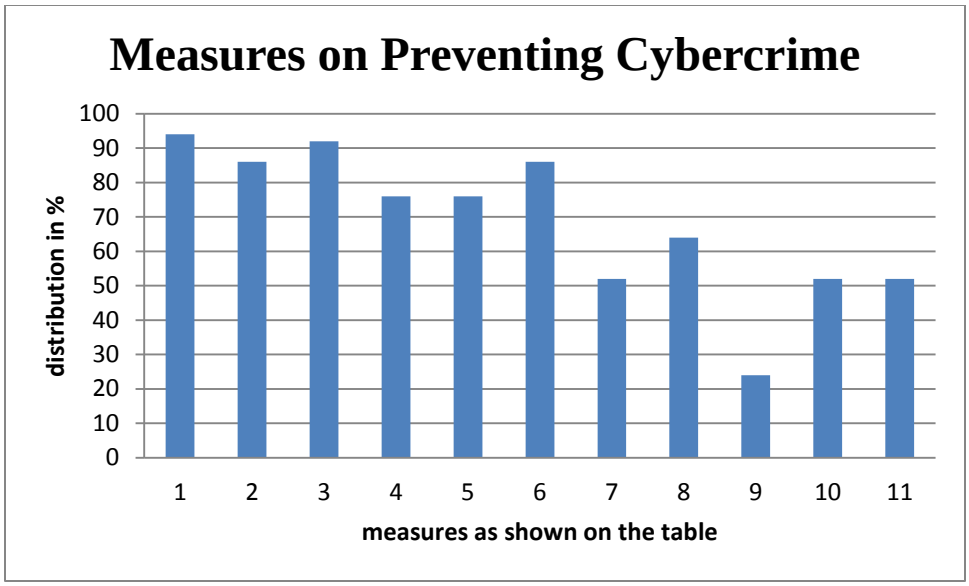



**Fig 5.2 showing measures on preventing cybercrime.**

| Key | % |
|---|---|
| **1. Antivirus** | 94 |
| **2. Software firewall** | 86 |
| **3. Antispam blocker** | 92 |
| **4. Data encryption** | 76 |
| **5. Data recovery strategies** | 76 |
| **6. Staff training awareness on cybercrime** | 86 |
| **7. Penetration testing** | 52 |
| **8. Bandwidth management** | 64 |
| **9. Hardware firewall** | 24 |
| **10. Customer behavior policies on cybercrime** | 52 |
| **11. Parental control software** | 52 |

# CHAPTER 6

## 6.0 SUMMARY AND CONCLUSIONS.

### 6.1 Summary.

This research has included all the methodology strategies for data collection as mentioned chapter three. Having examined and thoroughly analysed the collected data from all sources such as: primary sources, secondary sources, surveyor's questionnaires and observations, it has been clear to arrive at a precise conclusion to mark the end of this study.

### 6.2 Conclusions.

In line with the general objectives of the study, the following conclusions were arrived at.

Based on the results from data analysis and findings of the research, the study has revealed that cybercrime is silent but real as has been seen in most of the learning institutions. Due to that, the following conclusions were arrived at, based on the objective of the study; Firstly, it was observed that a number of cybercrime forms were prevalent in the Kenyan learning institutions most notably spamming, hacking, use of malicious code through viruses or Trojans. It means that if strategies will not be put in place then there is a great security risk posed through hacking, and cyber espionage where the learning institutions may stand to lose vital information or by having their websites denied access for instance, through denial of service attacks.

Secondly, the major focus on cybercrime employed by learning institutions was on providing means of curbing cybercrime that exist rather than finding ways of preventing them from occurring. As observed, currently spamming, hacking and phishing are at the forefront common forms of cybercrime employed by cyber criminals. Learning institutions especially, are purchasing expensive antivirus applications and firewalls to remove virus infections while ignoring preventive solutions such as, blacklisting specific IPs that are related to crime, which could be either phishing sites or even sites that are known to host viruses.

Thirdly and most importantly is that due to lack of awareness, ignorance and poor legislations have greatly contributed to slow progress against the fight on cybercrime. Furthermore, it is hard to convict cyber criminals because of two major reasons. Firstly,

our country has not enacted e-laws and the existing ones are not sufficient in convicting culprits because of jurisdiction anomalies. Secondly, obtaining evidence of computer crime that would stand in courts of law is lacking in our country since the field of computer forensics is still relatively new and lacks sufficient literature and expertise.

From the above it is clear, beyond reasonable doubt that if proper strategies are not put in place to curb cybercrime activities especially with the recent internet development, then Cybercrime will still continue to pose a great threat on security in the learning institutions.

## 6.3 Recommendations Limitations and Suggestion for Further Research.

### 6.3.1 Recommendations.

Prevention is the best solution to curb the increasing number of cybercrime trends in the Kenyan learning institutions. However, it may not be possible to prevent all incidents, and that is when two major factors come in play. Firstly, forensic knowledge and expertise, followed by the relevant laws that would empower victims to seek justice. This can be achieved through a number of measures discussed below.

There is a need for setting up a public facility i.e. a common site where victims can report incidences. The public need a lot of sensitization and training on what computer crimes are, in which forms they can manifest, how to detect them, what to do after detection and how to prevent and minimize them.

Legislative organs can mandate a body to filter all incoming web traffic before it is accessed by Internet users in the country and block away websites that pose security threats to the users. Internet Service Providers are also in position to protect their clients against most cyber-attacks like distributed denial of service attacks, email spoofing, spam that have become serious problem in most of the learning institutions.

### 6.3.2 Data loss prevention and information leakage.

In order to respond to data loss leakages problems, besides policies and procedures management can implement, Data Loss Prevention tools (DLP). It is an option that management can consider helping track sensitive information and help enforce policies. DLP tools are defined as

"products that, based on central policies, identify, monitor, and protect data at rest, in motion, and in use, through deep content analysis" (Mogull, 2009).

It should be noted that DLP tools most likely cannot stop "highly motivated threat agents" from within the organization, however, it can help "deter accidents, promote awareness and enforce information security and privacy policies by prompting the insider to exercise good information security and privacy practices" (Murphy, 2008)

There are three main components that a DLP tool works in order to protect data:

The first being the "data-at-rest" component, which actively "crawls" the servers, end-points and databases in order to find sensitive information and providing a snapshot of the different types of info in the network (Murphy, 2008).

The second component is called "data-in-motion", which is the actual monitoring and filtering of the network (Murphy, 2008). This component watches for any "tagged" sensitive information in the network traffic and enforces a policy if violation has occurred (Murphy, 2008).

The last component is called "data-in-use" which focuses on the endpoints, specifically workstations, laptops and end user activities (e.g. save to USB, print, save/save as, burn to CD/DVD. Policies are enforced at the end point if triggered, resulting in "prohibiting copy/paste, delete, e-mail, burning to CD, moving files onto USB stick, and printing" (Murphy, 2008).

### 6.3.3 Limitations

The greatest constraint in carrying out the research was time factor. Some of the respondents had little information hence giving out data which was not satisfactory and needed more input. Since most of the students are on session it was difficult to interact with the respondents most of time as they were held up in other areas. This made the research interviews to be limitedly carried out. It also took a while when collecting the questionnaires because some of the respondents kept them or even failed to reply to the questionnaire whereas some even discarded them up. There was also limited coordination and assistance from the supervisor as both of us were held up with the class work.

### 6.3.4 Suggestion for further research

Areas of further research that were identified include a similar study to be carried out on other sectors like the health sectors, financial sectors, and even the Kenya defense force sector. Crucially further research should be done to explore new techniques and procedures that will combat the rate at which cybercrime spreads and the ease at which they can be conducted.

## REFERENCES

A Study of Passwords and Methods Used in Brute-Force by Jim Owens and Jeanna Matthews Department of Computer Science Clarkson University.

ACC 626 IT ASSURANCE & GOVERNANCE-Information Leakage & Data Loss Prevention by Professor Malik Datardina (July 5, 2009)

Adomi, E.E. (2008). "Security and Software for Cybercafes," IGI, Global, USA.

An Analysis of Information Technology (IT) Security Practices: A Case Study of Kenyan Small and Medium Enterprises (SMEs) in the Financial Sector by Leonard Makumbi (School of Computing and Informatics University of Nairobi, Kenya), Evans K. (Miriti Lecturer, School of Computing and Informatics University of Nairobi, Kenya) and Andrew M. Kahonge (Lecturer, School of Computing and Informatics University of Nairobi, Kenya)

Bowling A (1997) Research methodology in Health- Bucking Open University press. Burns N and Croove .

Choo, K, R. (2011) The Cyber Threat Landscape: Challenges and Future Research Direction.

Combating current and emerging cybercrimes in Kenya (2011) by Fredrick Mugambi Muthengi Department of Computer Science Chuka University.

Combating current and emerging cybercrimes in Kenya (2011).

Criminal Investigations Department (CID), (January 2005)

Cybercrime and Computer Related Crimes Bill in Kenya

Cyberoam report, (2016)

Effects of Cybercrime on State Security, (2011).

Effects of Cybercrime on State Security: Types, Impact and Mitigations with the Fiber Optic deployment in Kenya- IBIMA Publishing-2011

Five Cyber Crimes on rise in (2015).

Five Cyber Crimes on rise in (2015).

Government of Kenya –cyber security strategy

Hemraj Saini, Yerra Shankar Rao, T.C.Panda / International Journal of Engineering Research and Applications (IJERA)

International Journal of Education and Research Vol. 3 No. 11 (November 2015) combating current and emerging cybercrimes in Kenya

International Journal of Education and Research Vol. 3 No. 11(November 2015).

International Review of Research in Open and Distributed Learning Volume 16, Number 1 Information Security breaches Survey Symantec data loss prevention industry overview (2015)

Julisch, K. (2013). "Understanding and Overcoming Cyber Security Anti- patterns."

Luo, X., & Liao, Q. (2007). Awareness Education as the key to Ransomware Prevention. Information Systems Security, 16(4), 195-202.

Mullers, Mervin E; Rezucha ,Iran(1962-06-01)Development of Sampling planby using sequential (item by item) selection Technique and Digital Computers.

Njoroge, C. K. (2008). "Director General, Communications Commission of Kenya.

Peisert, S., Margulies, J., Nicol, D. M., Khurana, H., &Sawall, C. (2014). Designed-in Security for Cyber-Physical Systems. Security & Privacy, IEEE.

Phenomena, challenges and legal response, (November 2014).

Philadelphia .W.B Saunders and Co.Likert R. (1932)

Poonia, A. S. (2014), Cyber Crime: Challenges and its Classification. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), ISSN, 2278-6856.

Poonia, A. S. (2014), Cyber Crime: Challenges and its Classification. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), ISSN, 2278-6856.

Report on - Dissecting the Top Five Network Attack Methods: A Thief's Perspective.

Romero-Mariona, J., Ziv, H., Richardson, D. J., & Bystritsky, D. (2009, April). Towards usable cyber security requirements. In Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies ACM.

Romero-Mariona, J., Ziv, H., Richardson, D. J., & Bystritsky, D. (2009, April). Towards usable cyber security requirements. In Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies.

S.K (1997) the practice of Nursing Research Conduct, Critique, and Utilization.

Scheier, F. (2012).On Cyber Warfare. DCAF Horizon 2015.

Summerville I., (2011), Software Engineering, 9th Ed. Pearson Education, Addison Wesley

Summerville I., (2011), Software Engineering, 9th Ed. Pearson Education, Addison Wesley

Sunter A.B (1977-01-01) - Random Sampling with equal or Unequal Probalistic without Replacement. Applied statistics.

Tashakkoriand Teddlie. Handbook of Mixed Methods in the Social and Behavioral Research. (2003).

Taylor, P. (1999). "Hackers: Crime in the Digital Sublime," Routledge, London

The Federal bureau of investigation (FBI) report (1995).

The Rise of the Cloud Security Professional Whitepaper, (2011).

Understanding cybercrime: Phenomena, challenges and legal response September (2012)

Understanding cybercrime: phenomena, challenges and legal response telecommunication Development Sector (September, 2012).

Vitter Jeffrey (1985-03-01) - Random Sampling with a Reservoir. ACM Trans. Math. Software.

White, G. B. (2011, November). The community cyber security maturity model. In Technologies for Homeland Security (HST), 2011 IEEE International Conference on (pp. 173- 178). IEEE.

White, G. B. (2011, November). The community cyber security maturity model. In Technologies for Homeland Security (HST), 2011 IEEE International Conference on (pp. 173- 178). IEEE.

**Appendix 1: Questionnaire**

**Questionnaire on the latest cybercrime trends in Kenyan learning institutions.**

Respondent Name (optional)…… Age……. Male…… Female……..

Level of study: Certificate… Diploma… Degree…

Questions

**Part (a)**

1. What is cybercrime?

……
……
……
……..

2. Are you aware of the cybercrime related cases? Yes… No…

3. Can your institution implement the security strategies within the available resources? Yes… No… Not sure…

**Part (b)**

1. Tick appropriately how frequent the listed cybercrime activities attacks you institution.

| Form of cybercrime | Very frequent | Frequent | Average | Rare | Never |
|---|---|---|---|---|---|
| viii. Spam mail | | | | | |
| ix. Denial of service | | | | | |
| x. Cyber stalking | | | | | |
| xi. Hacking | | | | | |
| xii. Cyber Espionage | | | | | |
| xiii. Phishing | | | | | |
| xiv. Others specify | | | | | |

Other form of cybercrime please add below

……
……
…….

3. Are users given prior notification from ICT about the cybercrime trends? Yes… No… Not sure…

**Part (c)**

1. What strategies have you employed to curb cybercrime in your institution? (Tick appropriately).

| | **Measures** | **Yes** | **No** | **Don't know** |
|---|---|---|---|---|
| **i.** | Antivirus | | | |
| **ii.** | Software firewall | | | |
| **iii.** | Antispam blocker | | | |
| **iv.** | Data encryption | | | |
| **v.** | Data recovery strategies | | | |
| **vi.** | Staff training awareness on cybercrime | | | |
| **vii.** | Penetration testing | | | |
| **viii.** | Bandwidth management | | | |
| **ix.** | Hardware firewall | | | |
| **x.** | Customer behavior policies on cybercrime | | | |
| **xi.** | Parental control software | | | |

2. What are some of the programmes in the learning institutions that are likely to suffer the consequences of the cyber-attacks?

A …….

B …….

C ……..

3. What is likely to be done in order to control all forms of cybercrime attacks in the learning institutions?

4. Give your general view on the impact likely to occur when cybercrime attacks are fully launched in the learning institutions ……

**Part d. 1. Cybercrime security implementation challenges.**

| | **To what extent do you agree with the following attributes in cybercrime security implementations in your institution (please tick as appropriate)** | Very Great Extent | Great Extent | Average Extent | Small extent | Very Small extent |
|---|---|---|---|---|---|---|
| **i.** | Your institution has adequate and sufficiently skilled personnel for cybercrime security management. | | | | | |
| **ii.** | Users are given adequate skills and awareness to support cybercrime security implementation. | | | | | |
| **iii.** | Resistance to change is an experienced in system security implementation in the institution. | | | | | |
| **iv.** | Your institution has adequate staff in order for cybercrime security implementation to be successful. | | | | | |
| **v.** | Refusal to use security strategies is experienced like limited user account rather than administrator. | | | | | |
| **vi.** | Incompatibility issues during installation of hardware firewall. | | | | | |
| **vii.** | Security software e.g. antiviruses, are evaluated during purchase, hence product work as planned. | | | | | |
| **viii.** | Change management training is conducted successfully during the Process. | | | | | |
| **ix.** | The implementation team always has sufficient experience and is able to set up the security systems properly. | | | | | |
| **x.** | Cost of the security implementation strategies overruns the budget. | | | | | |
| **xi.** | During the implementation staff sometimes ignore or refuse to stay on track to fulfill their responsibilities. | | | | | |

1. What are other factors do you think hindered the implementation process?

……
……
……

2. In your opinion what can the government do to aid in the prevention of cybercrime activities?

……
……
……

**Thank you for filling this questionnaire.**

Date …… Signature……..