THE IMPACT OF CYBERSECURITY IN ORGANIZATIONS IN KENYA.

NGIGI KIMANI JOSEPH

DICT/10/00042/2/21

A Research Project Submitted To The School Of Management and Leadership

In Partial Fulfillment for the Award of Diploma of Information and Communication Technology At the Management University of Africa.

AUGUST 2022

DECLARATION

This project is my original work and has not been presented for the award in any University or institution.No part of this research should be reproduced without the author's consent or that of Management University of Africa.

Signature…… Date…….

Joseph Kimani Ngigi

DICT/10/00042/2/21

This project has been submitted for examination with my approval as University supervisor of Management University of Africa.

Jefferson Maingi

Signature…….. Date……..

The Management University of Africa.

DEDICATION

This study is dedicated to my family for the constant support and encouragement throughout my study especially my dad Peter Ngigi and my mum Tabitha Wanjiru who have been there for me during the entire time of the study.

ACKNOWLEDGEMENT

I would like to thank the Almighty for the protection and the care he has given me since I started studying at the Management University of Africa.I also thank my beloved parents for the continued support they have showed when I have been at school since they provided me with everything that I required in order to make my learning more comfortable.I would also like to express my sincere gratitude to my supervisor Mr.Jefferson Maingi for his continued support and guidance during the research project writing.To my lecturer's,I express my sincere thanks for you have all contributed to the success of this project.Also to my friends who have been close to me I thank you all for your support,the information you all offered has been indeed of help to me in this research project,may the Almighty God shower blessing to you all.

I would like to acknowledge Secunets Technologies Ltd for letting me conduct this research at their premises.I am also expressing my sincere gratitude to the Management University of Africa for allowing me to pursue my education at the institution.

ABSTRACT

This study focuses on the impact of cybersecurity in Kenya, a case study of Secunets Technologies Ltd located at Kikuyu town.The objectives of the study were to determine how cybersecurity is an essential element to consider when setting up an organization.It is also to provide solutions to cyber attacks that may be experienced in organizations of they are not well secured.The attacks may include hacking of the organizations accounts, hacking their websites, phishing the organization's workers to get credentials that might lead to exploitation of the organization.During the study, I focused much on the manager of the institutions because the institution mostly deals with matters to do with cybersecurity, digital forensics, data recovery, web development, domain registration and also domain renewal.I also examined some few workers at the company whereby some were students who were being mentored by the CEO of the organization.The people there expressed the importance of cybersecurity in organizations whereby they were campaigning on the importance of securing your organization across the internet where organizations always face cyber bullying most of the time.The founder of the organization worked as a cybersecurity professional where he campaigned of the risks that are facing an organization that does not keep its systems safe from cyber attacks.I came to define that many attacks that are experienced in organizations especially large organizations happen through the internet for example hacking of the organizations compared to physical attacks for example when robbers rob organizations physically and take whatever they may require.The study defined that cyber security plays a major role in securing organizations from malicious attacks that might affect organization's computers, servers, mobile devices, electronic systems and also organization's data.The government should create awareness to all organizations by creating campaigns to show people the importance of cybersecurity in our nation.

TABLE OF CONTENTS

Contents

List of tables

Abbreviations

ICT:	Information and Communication Technology.
KICA:	Kenya Information and Communication Act.
ARPANETs:	Advanced Research Project Agency Networks
CMCA:	Computer Misuse and Cybercrimes Act.
MTD:	Moving Target Defense.
KE_CIRT/CC:	Kenya Computer Incident Response Team-Coordination Centre.
DDOS:	Distributed Denial of Service.

CHAPTER ONE

1.0 Introduction

This chapter presents background information of the study,statement of the problem,objectives of the study,the research questions,significance of the study and also the scope of the study.

1.1 Background of the Study

Cybersecurity is one of the most essential component to consider while securing your organization from malicious attacks.Many organizations today have advanced to using technology in making work easier.However cyber attackers have developed new ways and techniques so that they can be able to attack organizations over the networs of the organiztions.This might happen when for instance an attacker phishes an organization's system administrator and gets the logins to becomethe admin.With the logins to become the administrator,the attacker is able to control all the events that are undertake in the organization he/she has attacked. According to (Davies, 2021) cybersecurity began in the 1970s when researcher Bob Thomas created a computer programme called Creeper that could move across ARPANETs network(Advanced Research Project Agency Network which was the first public packet switched computer network)leaving a trail wherever it went.Ray Tomilson,the inventor of email wrote a programme Reaper which chased and deleted Creeper.Reaper was the first example of antivirus software.The cybersecurity industry is continuously growing at the speed of light.The global cybersecurity market size is forecast to grow to 345.4 bn by 2026 according to statista.Ransomware is one of the most common threat to an organization's data security and is forecast to continue to increase.The government is creating awareness to people on the importance of securing their organizations from malicious attacks because it has become the most common form of attack.Organization's accounts are hacked and a lot of important data is exploited and even money is grabbed from the accounts.

Table 1.1 Cyber threats detected.

Cyber threat events	Oct-Dec 18	Jul-Sep 18
Malware	6,026,924	1,844,897
Web application attacks	**737,289**	**1,064,971**
Botnet/DDOS	**453,371**	**911,298**
System misconfiguration	**3,449**	**2,548**
Online abuse	**158**	**252***

Source:National KE-CIRT/CC *Revised data.

According to Kenya Information and Communication Act(KICA),cybersecurity is defined as the collection of tools,policies,security concepts,security safeguards guidelines,risk management approaches,assurance and technologies that can be used to protect the cyber environment*(Thibault, 2014)*.To protect your systems and those of organizations,the government created various policies and laws namely Information and Communication Technology (ICT)policy 2020,Computer Misuse and Cybercrimes Act 2018(CMCA).The laws are important since Kenya has been reported to receive the second most cyberattacks after South Africa.

1.2 Statement of the Problem

According to *(Emm),* Kenya has been categorized as one of the countries that are being faced by cyber attacks at a high rate.The attacks have been as a result of lack of security in organizations and also lack of security in their networks.This study revealed that there is need for the government to offer training in order to make people understand the dangers of cyber attacks.The study is intended to express the importance of cybersecurity in organizations and also to express the importance of keeping your organizations secure from any attacks.The study is also bound to explain the consequences that are likely to occur if the security of an organization's network system is not guaranteed.

1.3 Objectives of the Study

The study was guided by the following objectives;

i. General objectives;

The general objective of the study was to demonstrate the impact of cybersecurity in Kenya.

ii. Specified objectives;

The specifieed objectives were as follows;

(i) To determine the different ways to keep organizations safe from attacks.
(ii) To determine the necessity of securing your organization from attacks.
(iii) To examine the challenges that an organization might face if their networks are insecure.
(iv) To examine the factors that have led to the increase of cyber attacks in Kenya.

1.4 Research Questions

(i) How does lack of knowledge among people in organizations affect cyber security.
(ii) How has the government helped create awareness to people about the importance of cyber security.
(iii) What roles have been undertaken by Information and Communication Technology specialists to control cyber crimes in Kenya.
(iv) Which are the laws and policies that have been set in order to control cyber attacks.

1.5 Significance of the Study

The findings of the study will provide a clear understanding on the importance of securing organizations from malicious attacks.The study will help equip knowledge to everyone that cyber attacks are common cases that have to be avoided in order to free your organization from risks.The study will also help the government to implement more laws and policies regarding cybercrimes and the actions to be taken if one is caught conducting a cyber attack.The research findings are also of help to the researcher because they will be able to create campaigns to

educate people on the importance of securing organization's networks and systems.Also the results of the study can be used for future research.

1.6 Scope of the Study

The research was carried out to determine the impact of cybersecurity in Kenya with reference to Secunets Technologies Ltd Kikuyu town.The target population was the companies CEO and also some workers at the organization who were also undergoing some training to become experts in the sector.It was assumed that the respondents would answer the questions asked willingly and honestly so that to get the right outcomes of the research.The study was conducted in the month of May to August year 2022.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

This chapter reviews literatures covered in an effort to address the impact of cybersecurity in Kenya.The chapter consists of the the theoretical literature review,empirical literature review,summay and research gaps,conceptual framework and operationalization of variables.

2.1 Theoretical Literature Review Error! Bookmark not defined.

Brief history of cybersecurity.

According to (Davies, 2021), cybersecurity began in the 1970s when Bob Thomas a researcher created a computer programme called Creeper that could move across ARPANET network

leaving a breadcrumb trail wherever it went.Ray Tomilson the inventor of email then wrote the programme Reaper which chased and deleted Creeper.The Reaper was the very first example of antivirus software making it the first ever computer worm.In 1987 the release of the first antivirus product occurred and was released by Andreas Luning and Kain Figge.By the 1990s people had started putting their personal information online and attackers saw this as a potential source of revenue and started stealing data from people and governments via the web.By the middle of 1990s,network security threats had increased so much that firewalls and antivirus programs had to be produced on a mass basis to protect the public.In the early 2000s,the government became serious on the matter on criminality of hacking,giving much more serious sentences to those caught doing the act.The cybersecurity industry is continuing to grow at high rate.The global cybersecurity market size is forecast to grow to 345.4bn by 2026.Ransomware is one of the most common threats to any organization's data security and is forecast to continue to increase (Davies, 2021). Due to the growth that has been taking place and the rapid increase of cybersecurit industry,the study has determined that few years to come,cases of cyber attacks will have lowered because people will be well conversant with how to secure their organizations.Also it has proven that there will be more and more attacks because attackers are still coming up with new inventions on how to trick and attack people.Therefore people should be careful when handling the internet or social media.

i. MTD system theory.

MTD stands for Moving Target Defenses. According to (Bardas) MTD theory is a form of computer security that eliminates the static nature of current computer systems.The MTD system theory can be thought simply as constantly changing a computer system to reduce or move the expoloitable attack surface.It defines MTD systems based on the concept of configurable system that is defined in terms of configuration parameters.The configuration parameters are used to capture the notion of the configuration units that a configurable system can control and is formalized as a value or name.An MTD can also take actions called adaptations that allow it to modify the values of its configuration parameters.Specifically adaptations are defined as a sequence of actions that change the system from one starting configuration state to another valid configuration state.Using MTD system,we define configuration space as the set of valid states in which an MTD system can exist.We also define the three key research problems related to MTD

systems.The MTD problem was defined as how to select the next configuration state of the MTD system.The adaptation selection problem was defined as how to select the adaptations to perform in order to get to the next configuration state.The timing prolem was defined as whe to carry out the adaptations to acually change the state of the system.

ii. Qualitative theory of cybersecurity.

According to (Fragkos, 2020) an extensive literature review and interviews with experts in the cybersecurity domain were the primary sources for this theory.The objective of this theory was to produce a qualitative casual theory to support assessments of cybersecurity vulnarability.To efficiently tackle practical issues related to cyber security assessments,the theory should offer a good tradeoff between the cost of applying the theory,cost of quantifying the theory and the theory's accuracy.First,literature was consulted to identify which attack steps to include.It included review oof a large number of textbooks,standards and reports,overview articles and security databases.

The qualitative theory was subsequently reviewed by domain experts.The reviews were made both on a high level of abstraction to ensure that the scope constituted a reasonable tradeoff and on a low level of abstraction to prioritize specific countermeasures and operationalize their definition.

iii. Quantitative theory of cybersecurity.

According to (Fragkos, 2020) the theory describes the relationship that needs to be quantified.A larger portion of the relationships could be quantified from the definition of constructs.Searches for data in literature were performed in article indexing services.They aimed at finding studies that contained data on the relationships specified in the qualitative theory.In order to produce a quantitative theory that could approximate the relationships,the judgement of domain experts was used.Experts in the scientific community were the primary reespondents in these surveys.However a number of practitioners were also included.A number of techniques has been suggested for combining expert judgement,including ;equal weight,consensus methods,peer recommendations and cooke's classical method.

iv. Securitization theory of cybersecurity.

According to (Huysman, 2006), securitization theory shows us that national security policy is not a natural given, but carefully designated by politicians and decision-makers. The general concept of „security" is drawn from its constitution within national security discourse, which implies an emphasis on authority, the confronting – and construction - of threats and enemies, an ability to make decisions and the adoption of emergency measures. The exact definition and criteria of securitization is constituted by the intersubjective establishment of an existential threat with a saliency sufficient to have substantial political effects. According to *(Denning,1999). I*nformation Warfare and Security. Reading, Massachusetts: Addison-Wesley 290-292), the history of cyber security as a securitizing concept begins with the disciplines of Computer and Information Science. Threats to cyber security do not only arise from (usually) intentional agents, but also from systemic threats. Threats arise from software as well as hardware failures and cannot be corrected through perfecting digital technology and programming, there is in short an inherent ontological insecurity within computer systems. Cyber security can in short be seen as „computer security plus "securitization".

Acccording to (Nissenbaum, 2008)*)*, key to understanding the potential magnitude of cyber threats is the networked character of computer systems. These networks control physical objects such as electrical transformers, trains, pipeline pumps, chemical vats, and radars and cyber disasters which would compromise systems and networks in ways that could render communications and electric power distribution difficult or impossible, disrupt transportation and shipping, disable financial transactions, and result in the theft of large amounts of money. According to (Nissenbaum, 2008), there is RANDs scenario which shows aptly how cyber security discourse moves seamlessly across distinctions normally deemed crucial to Security Studies: between individual and collective security, between public authorities and private institutions, and between economic and political-military security.

The theory encourages the privacy of ones cyber space where you should keep your space private and confidential so as to prevent attacks which might e brought about by exposure of your space. Securitization works in short by tying referent objects together, particularly by providing a link between those that do not explicitly invoke a bounded human collectively, such as „network" or „individual", with those that do. The securitization theory has simply been

playing a role of ensuring that you secure your cyber space from attacks. It is based on explaining the importance of being secure whereby when you secure your accounts, attackers will find it hard to attack their systems.

2.2 Empirical Literature Review

2.2.1 Lack of knowledge.

Knowledge is an important factor in every sector in Kenya today.For you to achieve a certain objective or goal,you first of all have to be well equipped with knowledge on the problem.In cybersecurity,lack of knowledge is one of the key elements that has led to the growth and development of cyber crimes.A example of Kenya today,many people are not well converant with the importance the security of their status on social media and across the internet.The people take it for granted and really don't care what might happen if they are hacked.Hackers might use their details to perform roberries in the name of the victim .This will lead to investigations whereby the victim might be sentenced for the hackers mistakes.But we have to ask ourselves why such cases happen in Kenya today.The reason is that people have not been well equipped with the knowledge of securing their personal data or anything.An example of knowledge that many people do not have is phishing *(wikipedia, the free encyclopedia)*.Many people have been phished in Kenya today and their personal data andinformation has been accessed by the attackers.It happens mostly when an attacker creates a malicious email and in the email the attacker attaches a link.The email is formulated in such a way that you cannot suspect anything or thinkthat it is from an untrusted source.The email is always convincing that you will have no doubt in clicking the link.Once you click the link you are done,it leads you to a website created by the attacker whereby you are asked to fill your credentials for example,usernames,passwords,bank account details and all sorts of personal information that the attacker might need.When you fill in the credentials,they are accessed directly by the attacker and now he has all your information.He can decide to rob your accounts in the case of a bank or use the data to blackmail you and make you offer payments to him.

An example of a phishing attack is;(An attacker sends an email pretending to be equity bank.The email says,"thank you for being our trusted customer and chosing us as your better option.We as

equity bank hope that you enjoy our services .We would like to inform you that we have made changes in our systems and we would kindly ask you to update your account details for security of your account.To do this,click on the link below www.equily.com.")That simple,you fall for the trap and all your data is accessed.The reason why this happens is because people have no knowledge based on cyber security.According to Secunets technologies Ltd,they have created a phishing campaign whereby they train people on how to avoid such scenarios.It is estimated that as time goes by,cyber attacks will otinue rising and so people have to be well equiped withknowledge on how to overcome or avoid the attacks.The government should also create learning programs to train people on the essentials of cyber security which will help in the growth of the field of cybersecurity.When this happened ,cyber attacks will be minimized and risks will be avoided.

2.2.2 Government Policy.

According to *(Mwangi, 2022),* the Kenya Information and Communication Act(KICA) 1998,mandates the Communication Authority of Kenya(CA) to develop a national cybersecurity management framework.The government established the National K(national KE_CIRT/CC) to ensure that there is a safer Kenyan cyber space.The KE-CIRT/CC is a multi agency collaboration framework whisch is responsible for the national coordination of cyber security as Kenya's national point of contact of cyber security matters.The government also enacted the Computer Misuse and Cyber Crimes Act of 2018 which has gone a long way in strengthening KE-CIRT/CC collaboration framework.The national KE-CIRT/CC coordinates response to cybersecurity matters at the CA centre and comprises of staff from Communications Authority and Law Enforcement Agencies.The functions of KE-CIRT/CC are as follows *(COMMUNICATIONS AUTHORITY OF KENYA);*

- ✓ Implementation of national cyber security policies,laws and regulations.
- ✓ Promote cyber security awareness and capacity building.
- ✓ Offer early warnings and technical advisories on cyber security threats on a 24/7 basis.
- ✓ Conduct researches and development in cyber security.
- ✓ Promote and facilitate the efficient management of critical internet resources.

The government has enacted laws that concern cyber security.Failure to follow the laws and adhere to them,there are consequences and charges for breakig the laws There is a sentence not less than 10 yearsin custody or a fine not exceeding 10 million kenyan shillings or both the fine and the sentence.We should follow the laws and strictly adhere to them failure to which the consequences are tough.

2.2.3 Information and Communication Technology.

According to *(Boulanin{PDF})*, Information and Communication Technologt (ICT) focuses on fudamentals of personal online security and safety.The ICT security measures are necessary to protect confidential information from unauthorised use,loss or release.It also monitors and controls confidential information, ensures safe data transmissions and also secures storage and disposal of data.Informatio and Technology (IT) plays a significant role in strengthening the national security against future upcoming threats and cyber attacks.It can help countries identify potential threats ,share information easily and protect the mechanisms in them.ICT provides potential for people to acquire skills and knowledge on cyersecurity and use the capabilities for their own interests and for the society also.Information and Communicatio Technology (ICT) department plays a great role in the field of cyber security in that it helps in protecting confidentia information from unauthorized usage.It also plays a great role in educating people on the need for securing information thus creates a pleasant cyber space for working.

2.2.4 Cyber laws and policies.

According to *(nelson, 2019)*, the cyber security field is guidedd by some laws and policies which have to be followed.There are rules that have been set and when they are broken,the victim will undergo some consequences.Generally cyber security n Kenya is to ensure the security of Kenya's cyber space and protect its users from attacks.The laws that govern the field should e adhered to failure to which there are penalties like sentences,heavy fines and others.Based on this study ,the reasercher focused on few cases of cyber crimes and the outcomes that follow when they are tampered with;

(i) Hacking (unauthorized access)

It constitutes a crime under section 14 of the Computer misuse and cyber crime act 2018.Its penalty upon conviction is a fine not exceeding KES 5 million,imprisonment for a term not exceeding 3 years or both.

(ii) Phishing

Phishing is identified as an offence under section 30 of the computer misuse and cyber crimes act and upon conviction it results to a penalty of KES 300,000 as fine,imprisonment of 3 years at maximum or both.

(iii) Infection of IT systems with malware.

The malwares include ransomware,spyware,worms,trojans and viruses.The offence entails causing interference to a computer system,program or data intentionally and without authorisation.The penalty upon conviction is a fine of not more than KES 10 million, imprisonment for not more than 5 years or both.

(iv)Possession or use of hardware,software or tools used to commit a cyber crime.

Under section 18 (2) of the computer misuse and cyber crimes act 2018,knowingly receiving or being in possession of a program or computer password,access code or similar data designed or adapted for commiting an offence,it constitutes an offence and upon conviction,there is a fine of not more than KES 10 million.

The few examples of punishment have been made so as to help reduce the acts of attacks so as to make attackers avoid conducting attacks. They are few among cyber security laws and have been enforced such that you cannot escape with it once you do the mistake.Cyber security field with help from the ICT department are doing their best to make sure the cyber attacks are reduced at a high rate.

2.3 Summary and Research gaps

Researchers have investigated the impact of cyber security in organizations in Kenya.It is evident in the literature review that lack of knowledge on the concept of cyber security is the mast factor that is leading to the increase of cyber crimes and attacks. To fill the gaps,the study conducted a further research in order to come up with the most appropriate way to make

everyone familiar with what cyber security really is and its usefulness.From a kenyan perspective,it is evident that kenyans are ignorant of this and so providing a better solution might be hard.The study sought to address these problems and it is evident that for there to be enough security of our cyber space,everyone should be equipped with the knowledge on cyber security and its importance in our cyber space.

2.4 Conceptual Framework

Conceptual framework illustrates what you expect to find through your research.It defines the relevant variables for your study and maps out how they might relate to each other.It is generally development on the basis of a literature review of existing studies about the topic.

Table 2.4 Conceptual framework.

Knowledge skills Equip people with knowledge about cyber security. **Government Policy** National KE-CIRT/CC to help in implementing laws. **ICT** Protect confidential information from unauthorized people. Educates people on importance of cyber security.	**Factors impacting cyber security.**

2.5 Operationalization of Variables

Table 2.5 Operationalization of variables.

Independent variable	Indicator	Measure scale	Instrument
Knowledge skills	Need for knowledge about cyber security by the people.	Ordinal	Questionnaire
Government Policy	Implementation of laws based on cyber security.	Ordinal	Questionnaire
ICT	Data protection. Offering cyber security education	Ordinal	Questionnaire

CHAPTER THREE

RESEARCH DESIGN AND METHODOLOGY

3.0 Introduction

This chapter includes the research design that gives the overview of the way this research was conducted,the target population,the sample and sampling technique,the instruments used in the study.It also explains the pilot study,data collection procedure,data analysis and presentation and ethical considerations.

3.1 Research design

A research design refers to the overall strategy that the researcher chose to define the different components of the study in a logical way thereby ensuring the research problem is effectively addressed.The researcher adopted a descriptive research design.The design is a type of research design that aims at obtaining information to describe a phenomenon, situation or population.The design helps to answer the questions what ,where ,when, and how regarding on the research

problem.The research involves gathering data,describing events and then organizes and tabulates the data collection.It was defined that descriptive study is used to generate specific objectives resulting in definite conclusions.The data collected in a descriptive research provides a base for further research sinde it helps obtain a comprehensive understanding of the research question so that it can be answered appropriately.

3.2 Target Population

According to *(Barnsbee 2018),* Target population is defined as the group of individual that the researchers intend to conduct their reserch on and draw conclusions from them.Target population simply means or is generally defined as a group or set of elements that you want to know more information about.The study targeted the total number of participants 30 ,15employees at Secunets Technologies Ltd and 5 investors in the company and 10 residents in Kikuyu town as depicted in the table below.

Table 3.2 Target Population.

Category	Target population	Percentage%
Top level management	1	3.33
Middle level management	14	46.67
Investors	5	16.67
Residents in the area	10	33.33
Total	**30**	**100**

3.3 Sample and sampling technique

When conducting a research in an organization,it might be very hard to study the whole population and therefore sampling is done.This is the selection of a subset of the population of interest in a research study.For Secuets Technologies Ltd,it is still a young and developing company with few workers and so the researcher was able to conduct the research with quite a good number of the company's population.

Table 3.3 Sample population.

Category	Target population	Sample population	Percentage%
Top level management	1	1	3.33
Middle level management	14	6	46.67
Investors	5	3	16.67
Residents of the area	10	8	33.33
Total	**30**	**18**	**100**

3.4 Instruments

A questionnaire is a list of questions or items used to gather data from respondents about their attitudes,experience or opinions based on the study (Bhandari, 2020).The data for this study was collected through the administration of questionnaires with structured questions.The questionnaires were derived from the study and highly dependent literature review of the study.This instrument was divided into two sections;section A was for general information from the respondents whereas section B was for specific questions.The researcher used both the open ended questions and also the closed ended questions to gather data from the respondents.

3.5 Pilot Study

Acccording to (In) A pilot study is the first step of the entire research protocal and is often a smaller sized study assisting in planning and modification of the main study.It may be used to predict an appropriate sample size of the full scale project and to improve upon various aspects of the study.Before a pilot study begins,the researcher must fully understand not only the clear purpose and question of the study,but also the experimental methods and schedule.A pilot study is performed either as an external pilot study independent of the main study or as an internal pilot study included in the research design of the main study.The study used a sample of 5 randomly selected respondents .The study pre-tested its questionnaires to establish its reliability and its validity.

3.5.1 Validity

Validity refers to how accurately a method measures what it is intended to measure *(Middleton)*.If the research has high validity,that means it produces results that correspond to the real properties,characteristics and variations.To enhance validity,the questionnaires were prepared in relation to the research objectives and in consultation with the university supervisor who approved the content.The main reason for validating the questionnaires wes to assess their appropriateness before conducting the research.

3.5.2 Reliability

According to *(Middleton)*, Reliability in research refers to how consistently a method measures something.If the same result can be consistently achieved by using the same methods,under the same circumstances,the measurement is considered reliable.The researcher conducted the study by administering the questionnaires twice to test the reliability.The study was found reliable because the same data was collected after conducting the research twice.

3.6 Data Collection Procedure

According to *(Bhandari)*, This is a process of gathering and collecting data and information to address a research problem.A closed and open ended design questions were used in the questionnaires to gather the information from the respondents.By using this two types of questions,both qualitative and quantitative were collected.The study obtained the necessary documents before commencing the research.

3.7 Data Analysis and Presentation

Data analysis is the process of developing answers to questions through the examination and interpretation of data.The basic steps in the analytic process consists of identifying issues,determining the availability of suitable data,deciding on which methods are appropriate for answering the questions of interest,applying the methods and evaluating,summarizing and communicating the results.The study adopted qualitative and quantitative data analysis.The data was tested and analyzed to determine its consistency and usefulness in the research process.The data collected was coded and this involved conversion of data into numerical codes representing measurements and variables.

3.8 Ethical Considerations

According to (Pedamkar), Ethical considerations are a set of principles that guide your research designs and practices.Also refers to the practices of how data is collected,stored and shared.They include ,how to safely store data or how to secure permissions to collect and use data.Ethics were highly considered in the study in that there was a high level of discipline and honesty while conducting the research.The selected respondents were informed about the purpose of the study before carrying out the data collection.

3.8.1 Informed consent

This was represented by an introduction letter from the researcher asking for permission to carry out the study. The participants had the right to accept or decline the offer for the study to be carried out in the organization.

3.8.2 Voluntary participation

The participants were informed about the purpose of the study before they made their decision,they were assured that the study was based for accademic purpose only.There was also the right for the participants to accept or reject the proposal.

3.8.3 Confidentiality

Respondents were given different names so that to keep them anonymous no to be discovered by anyone.They were adviced not to indicate their names anywhere in the questionnaires so that no one ca recognize them or have a clue about it.

3.8.4 Privacy

The study ensured that any respondent who participated in the research was entitled to privacy.The questionnaires were administered to the respondents in secure places where they felt they were safe and secure.The respondents privacy was highly valued.

ADDITIONAL FOR PROJECT

CHAPTER FOUR

RESEARCH FINDINGS AND DISCUSSION

4.0 Introduction

This chapter is comprised of presentation and research findings,and limitations of the study that is basically the challenges encountered during the study.This chapter also presents the data analysis methods and discuss them.

4.1 Presentation of Research Findings

From the 30 questionnaires issued to respondents, 18 of them were returned which is a 60% of the whole population and the rest were not returned which is 40%. From the 18 questionnaires that were returned, 3 did not have the appropriate feedback as per the study. The findings are depicted in the table below;

Table 4.1 Research Findings.

category	frequency	Percentage%
Returned	18	60
Not returned	12	40
Total	30	100

The finding from the above table shows that 60% of the respondents participated well and duly filled the questionnaire as required. 40% of the respondents did not return their questionnaires showing that they did not cooperate with the objective of the study. The respondents had the right to agree or deny filling the questionnaire because it was according to their own will and like.

4.1.2 Gender Analysis.

The research went ahead and sought out to find out the gender of the respondents and the following data was derived from the study.

Table 4.1.2 Gender Analysis.

category	frequency	percentage%
Male	12	66.67
Female	6	33.33
Total	18	100

The study findings shows that majority of the respondents were male whereby they were 66.67% while the females were 33.33%.This implies that males are more in the field of cyber security and also the cyber security welfare.

4.1.3 Age of the respondents.

The researcher aimed at finding the age of the respondents and the results depicted are as follows;

Table 4.1.3 Age Findings.

category	**frequency**	**percentage**
21-29	8	44.44
30-39	6	33.33
40-49	4	22.22
Total	18	100

The research findings determined that the young people aged between age gap 21-29 years are well conversant with the knowledge of cyber security. This has been proven by the research because according to it, they are leading with the largest percentage of 44.44%.This is because the generation now is more conversant with technological issues and are fast in learning many things within a short period of time. Those at the age of 30-39 years were 33.33% and those at the age of 40-49 years were only 22.22% thus proving that the knowledge of cyber security is well known to the young people that the elderly.

4.1.4 Knowledge skills.

The study sought to find out whether knowledge skills affect cyber security. Lack of knowledge is one of the factors that affect cyber security and it has led to the increase of cyber crimes in Kenya today. Many people lack knowledge on what effects would be brought by cyber attacks. People fail to know what danger would be acquired from lack of protection of personal data. This might lead to exposure of personal information and cyber attackers may use the information to ruin the reputation of the victims. Knowledge is an essential factor that may help reduce the rate of cyber attacks and it is required that everyone be equipped with the knowledge about cyber security. Once an attacker gains access to your account and you don't know about it, the attacker might perform all kind of things under your name and when noticed, you are the one who will be responsible of all the bad deeds committed because they are committed under your name. The research defined that knowledge should be spread all over to all Kenyans so that to explain to people on the importance of being cyber safe because it is more dangerous than physical attacks. The government should initiate campaigns in order to educate people and equip them with skills to help avoid cyber crimes and to minimize them. The government should also train experts to help in cases of cyber theft.

4.1.5 Government policy.

The government has a great role in the field of cyber security. The government should lead by examples in that they should secure their systems and protect them from attackers. The government has enacted laws and policies that are based on the cyber security field in which they should in which they should be followed by everyone. There is the Computer Misuse and Cyber Crime Act that was implemented by the government in order to discourage cyber crime and also to give the consequences of committing a crime. The government has set aside punishments that should be withheld once a person tries to break the rules. The act is in the constitution of Kenya and all the rules indicated in it should be followed to the later. There is also the Data Protection Act that was implemented by the government with the help of the Communication Authorities of Kenya whose purpose is to protect data of subjects (personal data) from being leaked or being accessed by any unauthorized personnel. The act states the rights of a data subject and the steps to be followed when collecting data from someone. A person's personal information is highly regarded and it should be handled with great care and not tampered with by anyone who is not authorized to access it. Subject's data should be highly guarded and protected because it can lead

to lots of damage and destructions if not well stored. The government should initiate campaigns in order to train people on how to keep their systems safe from attacks and also fund NGOs to help in training the public on how to keep safe from cyber attacks.

4.2 Limitations of the Study

The researcher encountered some challenges when collecting data such as the unwillingness of the respondents to cooperate in giving out the correct data according to the research. To address the issue, the researcher assured the respondents of their confidentiality for any information they gave. Some of the respondents did not fully trust the researcher and thus did not help in filling the questionnaires thus the case of incomplete questionnaire filling was experienced. Some respondents insisted to know the purpose of being questioned and demanded to know if the research was conducted in the official way and procedure and hence it took time to convince them. They also demanded to know the significance of the study. The researcher explained to the curious respondents on the significance of the study and he assured them that the questionnaires were meant only for academic purposes and would be kept confidential.

CHAPTER FIVE

SUMMARY, RECOMMENDATIONS AND CONCLUSIONS

5.0 Introduction

This chapter presents a summary on the summary of findings that were discovered during the study.It also presents a summary on the recommendations based on the research conclusions which can lead to addressing solutions on how to prevent cyber crimes.

5.1 Summary of Findings

5.1.1 Effects of lack of proper knowledge skills on cybersecurity.

From the research findings, majority of the respondents revealed that lack of knowledge skills about cyber security was a great issue that affected the country and the security of its cyber space. They indicated that many people had no knowledge about the importance of securing their systems and that's where the attackers take advantage and take control of them and use them to gain revenue from the affected victims. The study showed that if the government with the help of NGOs initiated trainings to train people of the essence of cyber security, the cases would be minimized. Even though the attackers are inventing new ways to attack the systems, with knowledge of the dangers we might face, it will help minimize the damage and the attackers will not be in a position to attack.

5.1.2 Effects of government policy based on cyber security.

From the research it is evident that the government has played a great role in the field of cyber security in many ways. One of them is that the government itself is acting as a good role model and it is protecting its systems not to be tampered with by the attackers. The government has employed specialists who help in keeping safe its systems and hence attackers have to face the specialists first before interfering with the systems. The government also has enacted laws that help govern the field of cyber security. The Computer Misuse and Cyber Crime Act is one of the policies that the government has implemented in order to fight for cyber security*(* (Mutinda)*)*. The Act entails rules on how to handle the internet and also the resulting punishments that may arise once the rules have been broken. The government has also enacted the Data Protection Policy where by it tends to protect the personal information of the people it is in charge of. It provides the rights of the data subjects that is the owners of the information and describes the safety measures of how their data should be handled.

5.1.3 Challenges affecting the field of cybersecurity.

According to *(* (al A. P.)*)*, As technology keeps on improving day by day, cyber security threats are also increasing day by day. Attackers are innovating new ways to attack systems and gain whatever they need. They try to come up with new ideas on how they can access information they might need from the target systems. One of the challenges in the field of cyber security is the evolution of ransomware. The last few years have seen a widespread rise in ransomware attacks. Ransomware can also be classified as one type of apt attack where malware penetrates

inside your system, and as the days pass, it starts to encrypt all of your files slowly. Finally, all the files on one's system get locked, and a ransom is being demanded, so that the encrypted data can be decrypted. Another challenge facing the cyber space is the IOT threats.IOT stands for internet of things. It is a system of interrelated computing, digital, mechanical devices that can transmit data over a network without the need of any human to human and human to computer intervention. Each machine has its own unique code that helps it to be identified and attackers use the codes to trace specific machines that they are targeting. Another challenge is cloud security. Many organizations are unwilling to put their data on the cloud, and they want to be reserved for a time unless it is ensured that the cloud is a highly secure place to store their data. The cyber security team is playing a hard role in convincing the people that it is safe to store the data there.

5.2 Recommendations

The study suggests the following recommendations;

The study recommends the government to join hands with NGOs and work hand in hand to help equip the people with knowledge skills about cyber security. The government should offer training centers and also hire some experts who will help equip people with knowledge about cyber security and how to prevent cyber attacks. It is also recommended that the computer systems of an organization should be scanned regularly with the help of antimalware software so that to ensure there is no threats in the systems which might have been imposed by the attacker. Also the government should strengthen the laws set aside for governing the cyber security field and whoever is found trying to break the rules by committing a cyber crime, a severe action should be taken on him or her. When all this is done, the cyber space will be safe to be accessed by anyone and cases of attacks will become scarce.

5.3 Conclusion

The study implies that the cyber security sector in Kenya is heavily affecting growth of organizations in Kenya in that whenever the organizations grow and get attacked, the start over again and it takes long to grow fully. It is clear from the findings that lack of knowledge skills on

cyber security has affected this field at a high rate whereby systems are tampered with without the knowledge of the users. The government should initiate programs and entrust them to some experts so that they can help in equipping people with the knowledge. The government should also introduce campaigns to fight against cyber crimes and train people on how to keep safe.

The study has also made it clear that the laws that govern the field of cyber security should be strengthened in order to prevent any form of cyber attack from happening. If it happens a heavy punishment should be taken upon by the government and with this the attackers will try and avoid such chaos. Also regular scanning of the systems to detect malwares should be done in order to make sure that the systems are free from any threat that could lead to them being attacked.

5.4 Reference

advisory, K. (n.d.). *Create value by haressing Risk*. Retrieved from The KMPG Advisory Services.The Trusted Imperative.: https://advisory.kmpg.us/articles/2021/risk-compliance-legal.html;//home.kmpg/governance

al, A. P. (n.d.). *These are the top cyber security challenges of 2021*. Retrieved from https://www.weforum.org/agenda/2021/01/top-cybersecurity-challenges-of-2021

al, C. o. (n.d.). *A look at the history of cyber security*. Retrieved from https://www.gcu.edu/blog/engineering-technology/look-history-cybersecurity

Algirde Pipikaite Lead, M. B. (n.d.). *Challenges affecting the field of cybersecurity*.

Archarjee, S. (2021, February 19). *Impact of cyber security an overview(2021)*. Retrieved from https://www.jigsawacademy.com/blogs/cyber-security/impact-of-cyber-security

Arkin, B. (2018, January 17). *The impact of public policy in cyber security*. Retrieved from https://adobe.com

Chang, J. (n.d.). *Cyber security statistics 2021/2022 Data and Market analysis*. Retrieved from https;financesonline.com/cybersecurity-statistics/

Cramer, A. (2016, December 12). *6 reasons why cyber crime is increasing*. Retrieved from Reasons why cyber crime is increasing and what can be done to prevent it: https://www.bmc.com/blogs/6-reasons-cyber-crime-increasing-can

Davies, V. (2021, October 04). *The History of cybersecurity.* Retrieved from http://cybermagazine.com

Fasano, E. (n.d.). *The biggest regulartory factors affecting cyber security budgets*. Retrieved from https://align.com

Foster, A. R. (2020). *Factors afecting risky cybersecurity behaviors by U.S workers:An explanatory study*. Retrieved from https://ScienceDirect.com

Goldsmith, J. (2007). *Factors affecting cybersecurity.* Retrieved from https://EssayGroom.com

Huysman, J. (2006). *The politics of Insecurity*. Retrieved from http://routledge.com

Information marketable for policy analysis of cyber-risks and trust. (n.d.). Retrieved from https://www.dhs.gov/science-and-technology/cybersecurity-impact

Javadi, M. A. (n.d.). *Cyber security challenged ahead pdf*. Retrieved from https://nexusacademicpublishers.com

M.Gilligan, J. (2017, September 19). *The government role in improving cybersecurity by John m.Gilligan* . Retrieved from https://The government role in improving cybersecurity-GCA/GLobal cyber alliance/working to eradicate cyber risk

Medromi, H. I. (2014, August). *The impact of cybersecurity issues on business and governments:A framework for implementing a cyber security plan*. Retrieved from https://researchgate.net

Mutinda, W. (n.d.). *The Computer Misuse and Cyber Crime Act 2018*. Retrieved from https://Kenya Computer Misuse and Cybercrimes Act,2018.Page 1. ICT Policy Africa

Nelson, O. (2019, June 13). *Cyber security laws.* Retrieved from https://cyberexperts.com/cybersecurity-laws

Nissenbaum, H. L. (2008). *cyber security and theories of cyber security: securitization theory*. Retrieved from https://cyberpolicy.blogspot.com

Pedamkar, P. (n.d.). *Challenges that are experienced in the field of cybersecurity*. Retrieved from cyber-security-challenges: https://www.educba.com/cyber-security-challenges

Poston, H. (2019, March 28). *Knowledge management on cybersecurity*. Retrieved from https://infosecinstitute.com

Report, 2. D. (2018). *New cyber threats*. Retrieved from What are the top factors affecting Cyber security strategy: https://esecuritysolutions.com

SAST. (2016, November 02). *How lack of knowledge affects cyber security*. Retrieved from https://the conversation.com/lack-of-cyber-knowledge-leads-to-lazy-decisions-from-executives-68065

Simplilearn. (n.d.). *top 8 cybersecurity skills you must have*. Retrieved from Cybersecurity skills you must have when in the field of cyber security: https://simplilearn.com

Stephen P.Mulligan, C. D. (n.d.). *The data protection act*. Retrieved from https://Data Protection Act of 2020/congress.gov/library of congress

Walsh, K. (2020, December 11). *CPRA hints at the future of cybersecurity and privacy*. Retrieved from https://help net security.com

APPENDICES

APPENDIX I: Introduction Letter

The Management University of Africa

P.O.BOX 29677-00100

Nairobi Kenya

Dear Respondent,

Re:Request for permission to carry out Research Study.

I am a student at the Management University of Africa and currently am conducting a research on the impacts of cyber security in organizations in Kenya.I am kindly informing you that you have been selected to assist in providing information since your points of view are considered very important in this study.Therefore I would urge you for your cooperation and participation during the study.You should also note that the information that you provide will be kept safe and confidential and be used for the purpose of the study.Thank you for the cooperation.

Yours sincerely,

Joseph Kimani.

APPENDIX II: Questionnaire / Interview Guide / Observation Guide/ Document Analysis Guide

The purpose of the questionnaire is to gather information on a research problem on the impact of cyber security in Kenya in specific reference to Secunets Technologies Ltd.The data provided will be used for academic purposes only and will be kept safe and secure.Your response is highly regarded and will be kept confidential.

SECTION A:Personal Information.

To indicate that you have answered the questions,tick where appropriate.

1.Gender

Male { }

Female{ }

2.Age Bracket

21-29 {}

30-39 {}

40-49 {}

Section B: Knowledge skills.

3. What knowledge skills is someone supposed to have so that they can avoid cyber threats?

.....

4. Where should one acquire the knowledge skills?

…….

5. How does knowledge affect cyber security?

…….

6. Is knowledge an important factor in cyber security impaction?

……

6b. Give a reason to your point of view.

……. . . . .

Section C: Government law and policy

7. How has the government policy helped build the field of cyber security?

……..

8. Should the government strengthen the policies to prevent cyber crimes?

……..

9. How has the government helped in building and securing the cyber space?

……..

10. Does the government need the help of NGOs in fighting against cyber crimes?

Yes {}

No {}

11. Based on your point of view, explain why you think it is appropriate or not.

……..

12. What do you think could be a solution to solving the problem of cyber crimes?

……..

13. What should the workers in organizations do in order to help in solving the problem of cyber crimes?

…….

14. Is it necessary for conducting scans on your computer systems?

Yes {}

No {}

14b.Give a reason to support your answer in a above.

……..

14c.After how long should scans be conducted on the systems?

…….

APPENDIX III: Time Schedule

Time schedule is the arrangement of the events from the moment of planning of a research study until the time it is conducted and the required feedback is obtained. It shows the different events that have been planned and the time allocated for them to be done. The following was the researcher's time schedule after Secunets Technologies Ltd allowed him to conduct the research in their company.

Table 5.1 Time schedule.

Weeks	Events
Week 1-2	✓ Learning what the company offers. ✓ Studying the company's websites to know the kind of services they offer. ✓ Asking and seeking more information about the company and how it deals with matters based o cyber security from the workers there.
Week 3-4	✓ Start using tools used by the company in cyber security. ✓ Received trainings on how to secure your systems from cyber attacks.
Week 5-6	✓ Administering questionnaires to workers to fill them so that to gain more knowledge because there are more experienced in the field. ✓ Conducting some scans on computer systems using antimalware software so as to detect malwares and threats that might be affecting the systems.
Week 7-8	✓ Combining all the information gathered in the research at the company. ✓ Analyzing the information and keeping it in rerecords ready for presentation. ✓ Presentation of the collected information from the research.

APPENDIX IV: Budget

A budget is a detailed statement outlining estimated project costs that support a sponsored project. It should include all the direct costs, as well as the calculated facility costs required to carry out the project objectives. The proposal budget should be derived directly from the project description and serves as the financial expression of the project. It follows some procedure so that to come up with the actual plot of the funds that were used during the study. If you are applying for funding, you must say what you are planning to spend that funding on. More than that, you need to show how spending that money will help you to answer your research question**.**

- I am going to conduct a research about cyber security in Kikuyu at Secunets Technologies Ltd.
- I will need a teaching release for three months for fieldwork.
- I will need transport money to take me to the place.
- I will also need money in order to cater for the rent of the place where I will be staying for the three months.
- I will also need enough money to print questionnaires that will be answered by respondents.
- I will need enough money to cater for my expenses such as food for the few months.
- I will need money so as to purchase data so that I can access the internet for more research.

APPENDIX V: Other Documents or Information Types

CYBERSECURITY CHALLENGES AND THE WAY FORWARD.

1. What is cyber-crime?

According to *(Nureni)*, It is any harmful act committed from or against a computer or network either to generate profit from them or to completely damage or disable them. It can also be referred to as computer crime. According to *(Director of Computer Crime Research Centre (CCRC) during an interview on the 27th April, 2004)*, It can also be defined as any illegal behavior directed by means of electronic operations that target the security of

computer systems and the data processed by them. It involves committing crime against computer systems or the use of the computer in committing crimes.

2. **Categories in which cyber-crime is divided.**

i. Cybercrimes against persons.

The cybercrimes committed against persons include various crimes like transmission of child-pornography, harassment of the computer user, trafficking, posting and dissemination of offensive material including pornography and indecent exposure. This is one Cybercrime which threatens to undermine the growth of the younger generation and also leave irreparable scars and injury on the younger generation, if not controlled. This harassments can be either sexual, racial or religious and persons caught performing such kind of harassments are also guilty of cybercrimes.

ii. Cybercrimes against property.

These crimes include computer vandalism (destruction of others' property), transmission of harmful programs and unauthorized possession of computerized information.

iii. Cybercrimes against government.

Cyberterrorism is one distinct kind of crime in this category. The growth of internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international governments and also to terrorize the citizens of a country*(. Gupta, CBI)*. This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website. Cracking is amongst the gravest Cyber-crimes known till date. It is a dreadful feeling to know that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information. Cybercrime can be broadly defined as a criminal activity in which computer or computer networks are a tool, a target or a medium for the crime.

3. **Types of cybercrimes**.

- ✓ **Unauthorized access of hosts (Hacking) -** Hacking can take various forms, some of which might not always involve deep technical knowledge. Social engineering involves “talking” your way into being given access to a computer by an authorized

user. The hackers are divided into two whereby there are those who break into computers with malicious intent or to sell information gathered from the compromised computer who are known as "*crackers or black hats*" and also those who do it out of curiosity or to enhance their technical ability known as "*hackers or white hats*".

- ✓ **Computer fraud /"Phishing" scams –**They involve a level of social engineering as they require the perpetrators to pose as a trustworthy representative of an organization, commonly the victim's bank. Phishing greatly occur using mails which the attacker uses to convince the target that it is from a trusted source.
- ✓ **Spamming –**It involves mass amounts of email being sent in order to promote and advertise

  products and websites. Email spam is becoming a serious issue amongst businesses, due to the cost overhead it causes and also the amount of time spent downloading/eliminating the spam mail. Spammers are also devising advanced techniques to avoid spam filters such as abandoning the use of email contents and use of imagery that cannot be detected by spam filters.
- ✓ **Denial of service attacks (DoS)-** It involves large volumes of traffic being sent to a host or network, rendering it inaccessible to normal users due to sheer consumption of resources. Distributed Denial of Service attacks involve multiple computers being used in an attack, in many cases through the use of "zombie" servers, which are infected with Trojan programs that attackers install on various computers. Often legitimate computer users have no idea they are involved in denial of service attacks due to the stealthy nature of the zombie software.
- ✓ **Viruses, Trojans and Worms**-They are software designed to "infect" computers- or install themselves onto a computer without the users permission. Many computer users have experienced the frustration of having a malicious virus wreck havoc upon their computers and data, but not all viruses have a malicious payload. Trojan is a program that allows for the remote access of the computer it's installed on. Worms make use of known vulnerabilities in commonly used software, and are designed to traverse through networks.
- ✓ *Violation of operation rules of computers, computer system or networks.*

- ✓ *Unlawful access to computer information.*
- ✓ *Creation, use and distribution of malware or machine carriers with such programs.*

4. **Causes of cybercrimes.**

- ✓ **Cybercrimes can be committed for the sake of recognition.** This is basically committed by youngsters who want to be noticed and feel among the group of the big and tough guys in the society. They do not mean to hurt anyone in particular; they fall into the category of the Idealists; who just want to be in spotlight.
- ✓ **Cybercrimes can be committed for the sake of making quick money.** This group is greed motivated and is career criminals, who tamper with data on the net or system especially, e-commerce, e-banking data information with the sole aim of committing fraud and swindling money off unsuspecting customers.
- ✓ **Cybercrimes can be committed to fight a cause one thinks that they believe in.** This is the most dangerous of all the causes of cyber-crime. Those involved believe that they
- ✓ are fighting just a cause and so do not mind who or what they destroy in their quest to get their goals achieved. These are the cyber-terrorists.

5. **How to eradicate cyber-crime.**

Research has shown that no law can be put in place to effectively eradicate the issue of cyber-crime. Attempts have been made locally and internationally, but these laws still have shot- comings. The challenge of cyber-crime can be fought more easily by education not laws. It has been proven that the education of idealists help big companies and government see security holes which career criminals or even cyber-terrorist could use to attack them in future. Most often, companies engage them as consultants to help them build solid security for their systems and data. The Idealists often help the society: through their highly mediatised and individually harmless actions, they help important organizations to discover their high-tech security holes. Another means of eradicating cyber-crime is to harmonize international cooperation and law, this goes for the greed motivated and cyber-terrorists. They cannot be fought by education, because they are already established criminals, so they cannot behave. The only appropriate way to fight them is by enacting new laws, harmonize

international legislations and encourage coordination and cooperation between national law enforcement agencies.

6. **Those involved in cyber-crimes.**

Those involved in cyber-crimes are divided in three categories that is;

a. **The idealists (Teenagers) -** They are usually not highly trained or skillful, but youngsters between the ages of 13 – 26 who seek social recognition. They want to be in the spotlight of the media. Most often they attack systems with viruses they created.
b. **The Greed-Motivated (Career Criminals)** - This type of cyber-criminals is dangerous because they are ready to commit any type of crime as long as it brings money to them. They are usually very smart and organized and they know how to escape the law enforcement agencies. These cyber-criminals are committing grievous crimes and damages and their effects are a serious threat to the society.
c. **The Cyber-Terrorists -** They are the newest and most dangerous group. Their primary motive is not just money but also a specific cause they defend. They usually engage in sending threat mails, destroying data stored in mainly government information systems just to score their point. The threat of cyber-terrorism can be compared to those of nuclear, bacteriological or chemical weapon threats. The disheartening issue is that they have no state frontiers; can operate from anywhere in the world, and this makes it difficult for them to get caught.

7. **The scammer tools.**

A combination of social engineering and programming skills are the most potent tools in the hands of the scammers. In order to reach a large volume of users, the scammers require an equally large number of email addresses. These are usually collected by using programs known as

spam-bots to search for email addresses listed on web sites and message boards by purchasing address lists from individuals or organizations. Once they have addresses, spammers can use programs known as “bulk mailers” to automate the sending of spam which can send huge volumes of email messages effectively hiding the true address of the spammer. Another popular method employed by scammers is the use of dating sites as a powerful tool to get attention and e-

mail addresses. A number of victims have fallen victim to dating scams. Another technique spammers utilize to send emails is with the use of zombie networks, also known as bot networks. Zombie is the term given to a computer that has been infected by a virus, worm, or Trojan , which allows remote entities to take control and use it for their own (usually illegal) purposes. This technique is also popular as it protects the identity of the spammer.

APPENDIX VI: Progress Report Record

A progress report is a written record of what has been done and what is left to do on a project. In other words it is a report of the progress that has been made on the project.

Table 5.2 Progress Report Record.

Weeks	Events
Week 1-2	✓ Learning what the company offers. ✓ Studying the company's websites to know the kind of services they offer. ✓ Asking and seeking more information about the company and how it deals with matters based o cyber security from the workers there.
Week 3-4	✓ Start using tools used by the company in cyber security. ✓ Received trainings on how to secure your systems from cyber attacks.
Week 5-6	✓ Administering questionnaires to workers to fill them so that to gain more knowledge because there are more experienced in the field.

Week 7-8	✓ Conducting some scans on computer systems using antimalware software so as to detect malwares and threats that might be affecting the systems. ✓ Combining all the information gathered in the research at the company. ✓ Analyzing the information and keeping it in rerecords ready for presentation. ✓ Presentation of the collected information from the research.