UNIVERSITY OF NAIROBI

COLLEGE OF BIOLOGICAL & PHYSICAL SCIENCES

SCHOOL OF COMPUTING & INFORMATICS

SOCIAL ENGINEERING IN E-COMMERCE PLATFORMS IN KENYA

LAWRENCE MWAGOTI MWASAMBO

P54/73325/2014

SUPERVISOR: MR. CHRISTOPHER MOTURI

A project report submitted in partial fulfillment of the requirements for the award of Masters of Science in Information Technology Management of the University of Nairobi.

OCTOBER 2016

Declaration

I declare that this project report is my original work except where due references are cited. To the best of my knowledge, this it has not been submitted for any other award in any University. Data from other sources has been acknowledged.

Sign_____**D**ate_____

LAWRENCE MWAGOTI MWASAMBO

Reg. No: P54/73325/2014

SUPERVISOR

This project report has been submitted in partial fulfilment of the requirement of the Master of Science Degree in Information Technology Management of the University of Nairobi with my approval as the University supervisor.

Sign_____ Date: _____

MR. CHRISTOPHER MOTURI

Dedication

To my Great parents and my extended family for their support and patience while undertaking this research.

Acknowledgements

First, my gratitude goes to our Almighty God for His mercies and grace that have enabled me to come this far.

I wish to express my sincere gratitude to my supervisor, Mr. Christopher Moturi, for his immeasurable guidance, support, encouragement and time input that enabled my research and write this thesis report, Dr. Orwa, Professor Wagacha, Dr. Ruhiu for their valuable input into my work. To all my lecturers in the MSc. Information Technology Management course for impacting knowledge and academic rigor to me. Lastly all MSc SCI lecturers, colleagues and staff of the University of Nairobi – School of Computing and Informatics for the assistance extended to me in one way or the other.

May the Almighty God bless you all.

Table of contents

Abstract

Cyber criminals have extremely targeted eCommerce as they receive and use money, relay in technology, outsourced services and use of payment technologies like mobile money and online banking channels to carry out their day-to-day transactions. Criminals have shifted to use of social engineering as it easy to exploit user's natural inclination as compared to hacking. This research was based on mixed research methodology whose aim was to seek an in-depth understanding of concerns and mitigation approaches of social engineering in eCommerce platforms in Kenya. Purposive sampling was used and a sample size of 30 eCommerce organizations. Data was collected using questionnaires from IT managers and business managers. The questionnaires were created based on the four dimensions of Social Engineering Defensive Framework. Social engineering mitigation best practices are proposed. This report concludes by emphasizing the need of organizations using the derived best practices and incorporating security culture.

List of Abbreviations

B2B- Business-to-business eCommerce

B2C- Business-to– customer

B2G- Business-to-government

C2B- Customer-to–business

C2C-Customer-to-customer

CAK- Communication Authority of Kenya

Cert-UK-Computer Emergency Response Team- United Kingdom

FBI- Federal Bureau of Investigations

G2B-Government-to-business

IC3- Internet Crime Complaint Centre

IFMIS- Integrated Financial Management Information System

M-pesa- Mobile Money Transfer Service

OLX- OnLine eXchange

PII-Personal Identifiable Data

SDVAs- Social-driven vulnerability framework

SMTP-Simple Mail Transfer Protocol

SEDF-Social engineering defensive framework

SEPF- social engineering personality framework

SE-Social Engineering

WTO- World Trade Organisation

List of Tables

List of Figures

CHAPTER ONE
INTRODUCTION

1.1 Overview

This chapter gives background information on information security, provides an overview of eCommerce, and elucidates the research problem, objectives, hypotheses, justification and finally scope and limitations of the study.

1.2 Background Information

"Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities,"(Abraham & Chengalur-Smith, 2010; Koteswara & Janczewski, 2014). Information Security provides a basis, from which threats to information systems can be identified, analysed and crafting combating strategies to the identified threats. With the said strategies in place, still, organizations face a big challenge from sophisticated attacks which are being remodeled by attackers with every strong and new protective measure deploy to ensure their network security is adequately maintained. Attackers have now diverted their attacks from old-fashioned security models of attacking hardware and software, to end-users of information systems; which form the weakest link in computer security. As Luo, Brody, Seazzu, and Burd (2011) found "a plethora of technological methods has been developed to address various security issues but human factors that contribute significantly to security breaches have been comparatively neglected," . Mulwa (2012) found out that with the present dynamic technological developments, electronic information has grown in significance, businesses now conduct most of their day-to-day business undertakings electronically and this has drastically changed the level of information security threat.

CAK (2015) " third quarter sector statistics report for the financial year 2015/2016 shows that the internet/data market has maintained an upward trend with the quarter review registering 24.7 million up from 23.7 million subscriptions recorded the previous quarter and internet users stood at 37.4 million up from 35.5 million users estimated during the quarter which translated to internet penetration levels of 87.2 percent." The dawn of the internet saw entrepreneurs all over the world capture the idea and infuse technological innovation to create new produce, services and business models (Hasan & Harris, 2009; Kabuba, 2012), giving purely internet-based companies now regularly referred to "internet based" or "online

company" a name that is applied to a company that conducts most of its business online , since that business engage physical logistics systems. This trend has been exhibited in Kenya, where many businesses are now adopting eCommerce due to eased shopping hence making it more convenience and thus more appealing to the large population which accesses internet services in Kenya.

Table 1:Internet subscriptions and Internet Users(Source: Communication Authority of Kenya Third Quarter Sector Statistics Report for the Financial Year 2015/216(January-March 2016))

Internet/Data Subscriptions	***16-Mar***	***15-Dec***	***Quarterly Variation (%)***	***15-Jan***	***14-Dec***	***Quarterly Variation (%)2***
Total Internet Subscriptions	24,848,065	23,929,657	3.8	18,802,428	16,453,019	14.3
Mobile Data Subscriptions	24,708,551	23,794,550	3.8	18,682,921	16,338,990	14.3
Fixed Wireless Data Subscriptions	13,792	19,507	-29.3	836	712	17.4
Satellite Data Subscriptions	299	489	-38.9	836	712	17.4
Fixed DSL Data Subscriptions	2,961	3,732	-20.7	14,685	14,512	1.2
Fixed Fibre Optic Data Subscriptions	122,437	111,354	9.9	87,838	81,243	8.1
Fixed Cable Modem Subscriptions	25	25	0	25	25	0
Estimated Internet Users1	37,418,671	35,549,620	5.3	29,158,301	26,163,560	11.4

Kigen et al. (2015) found social engineering as the second top cyber security issue in Kenya in 2015 after data exfiltration. Data exfiltration happens when data is copied and transferred without consent. Organizations overall commercial enterprises in Kenya are continually reporting a heightening in an assortment of innovative complex social engineering assaults. This is a reasonable sign of the prevalence of these violations and the failure of organizations to terminate them. With social engineering being propagated using advanced technologies, no extensive research has been conducted, particularly to Kenyan eCommerce platforms which have provided a futile solution and hence this threatens the integrity of eCommerce organizations and their customers.

1.3 eCommerce

There is no pact on the accurate meaning of eCommerce with various distinctive definitions being utilized as a part of different perspective. eCommerce has been described as " the sale or purchase of goods or services conducted over computer networks by methods specifically designed for the purpose of receiving or placing of orders, even though payments and actual delivery of goods and services do not have to be conducted online," (WTO, 2013). Kinuthia and Akinnusi (2014) described eCommerce as "conducting commercial activities via electronic media, and most commonly the internet." Mutuku and Kyalo (2015) defined eCommerce as "a way of conducting business by companies and their customers performing electronic transactions through computer networks." It is clear from the assortment of definitions offered that the key properties of eCommerce identify with all innovation-mediated exchanges between business parties, what's more, an arbiter, diverse types of electronic media are engaged in some point to enable such trades (Kabuba, 2012; Kinuthia & Akinnusi, 2014; Mutuku & Kyalo, 2015; Victoria, 2013; WTO, 2013).

Concentrating on the different parties involved there are different models of eCommerce, some of the most widely recognized are discussed here: Business-to-Business (B2B eCommerce) refers to the extensive spectrum of activities that happen between the two establishments and which by far is the most common (Kabuba, 2012), the principle segments of this idea are e-infrastructure, (which guarantees the base prerequisites identified with logistics and working programming) and e-markets, or sites that capacity as virtual meeting places where purchasers cooperate with bidders (Mirescu, 2011). Business-to-Customers (B2C eCommerce) includes retailing exchange between organizations and people or its customers, the primary markets are the retail (or e-tail) and e-banking (Online budgetary instruments designed for personal finance management) platforms(Mirescu, 2011). Consumer-to-Business (C2B eCommerce) which allows shoppers to provide items and administrations to organizations, an instance is independent sites like taskrabbit.com, any business organization that is occupied with conveying the managements of the purchaser can contact him and provide him the chance (Kabuba, 2012; Victoria, 2013). Business-to-government and government-to-business (B2G/G2B) represents the routes in which business transactions takes place between organizations and public sector, Mirescu (2011) found out that in the basic case, organizations complete exercises for the advantage of the public sector (obtainment contracts, barters, and so on.) while through G2B the public institutions are

predominantly educating the private sector about the legal framework or participation opportunities with them. In summation to the models discussed so far, there is Consumer-to-Consumer (C2C) model which is the character of trade between buyers and individuals, or buyers with other buyers.

1.4 Problem Statement

eCommerce is extremely targeted by cyber criminals as they receive money and due to their reliance on technology and third parties to perform and enhance their management and carrying out of daily transactions. With payment technologies like mobile money and online banking channels being engaged, these carry with them inherent risks as they expose previously closed presses to the internet. Criminals use social engineering tactics because it is more comfortable to exploit one's natural tendency to believe than it is to find ways to hack the software.

This academic research study seeks to investigate social engineering and it's mitigation in eCommerce platforms in Kenya. The study seeks response for the following questions: What are the different types of social engineering faced by eCommerce platforms in Kenya? What are the mitigation strategies to social engineering?

1.5 The study objectives

The objectives of this study were:

I. To identify social engineering risk in eCommerce platforms
II. To evaluate social engineering risks in eCommerce platforms in Kenya
III. To come up with social engineering risk mitigation best practices

1.6 Hypotheses

H1: Social engineering training will lead to reduced attacks on eCommerce platforms

H2: Social engineering training will bear no issue in containing threats and attacks in eCommerce platform

1.7 Justification of the Study

This study will assist eCommerce organizations to safeguard themselves against social engineering attacks, threats, and fraud. It will add value to the existing body of knowledge in developing an insight of social engineering mitigation and reduction in all the players in eCommerce platform.

CHAPTER TWO

LITERATURE REVIEW

2.1 Overview

This chapter presents a review of the related literature on the subject of Social Engineering as presented by various researchers and scholars. This chapter covers SE concepts, SE in global, Africa and in Kenya, SE threats in eCommerce Platforms, SE frameworks, conceptual framework and lastly operationalisation of research variables.

2.2 Social Engineering Concepts

A collective fallacy people devise about cyber attackers is they solitary use innovative hacking implements and tools to hack computers, and systems (Torres, 2014). This is false as attackers have discovered the easiest ways to rip-off information or hack PC is by just talking and deceiving the system users in order for them to disclose their valued credentials or information leading to some breach of security and loss of information. Koteswara and Janczewski (2014) found that "When people talk about information security, it's very common to think about threats that can be contained with the help of technical countermeasures such as email filters, network filters, anti-viruses and likes; however, there is a more elusive form of danger to which there in no obvious solution." Social engineering attackers, overall, " Tend to exploit human cognitive biases, attacks are non-technical intrusions that rely on human interactions, potentially bypassing technological security measures," (Luo et al., 2011).

R.Strozer et al., (2014) defined "Social engineering in context of information security, as the manipulation of people to get them to unwittingly perform actions that cause harm (or increase the probability of causing future harm) to confidentiality, integrity and availability of the organization's resources, including information, information systems or financial systems." Cert-UK (2015) defines social engineering as " The manipulation of individuals in order to induce them to carry out specific actions or to divulge information that can be of use to an attacker." Luo et al. (2011) described social engineering as "A combination of techniques used to manipulate victims into divulging confidential information or performing actions that compromise security." The effective or ineffective efforts to sway an individual(s) to both expose information or increases chances of corollary in illegal access, unlawful usage of, or unapproved revelation of an information system and its information

(Oosterloo, 2008). Basically, social engineering is what has been around the world throughout the generations, but today being applied through sophisticated means and purpose of current technologies in space.

2.3 Social Engineering in Global Perspective

ProofPoint (2016) found that social engineering become the number one attack technique in 2015. Attackers have deviated from computerized manoeuvres and rather engage individuals to execute their ploys of poisoning systems, pillaging credentials and relocating resources. In all the attacks and ploys of different magnitude, social engineering is used to lure persons into undertaking effects that were once determined by the use of infectious programs. Attackers employ individuals in three continuously guiding ways: executing attacker's code on their behalf unknowingly, handing over credentials to them or directly acting for them, transferring funds to them.

The FBI (2015) through Internet Crime Complaint Centre(IC3) released a public service announcement on the update for the business e-mail compromise, which is a refined scam zero in on companies with overseas traders or traders who often use electronic funds transfer. The scam is perpetrated through compromising authentic business electronic mails using social engineering ploys. According to the data, it indicates that business e-mail compromise remains growing targeting all businesses. The scam has been testified in all the fifty states in the US and in 79 more countries across the globe resulting businesses to a loss of $1.2 billion.

A research report by Verizon (Team, 2015), while conducting phishing campaigns noted that phishing statistics went higher, with 23 percent of receivers of phishing messages opened them and 11 percent clicked on the payloads as compared to previous year. The researchers noted in an operation of 10 electronic mails yielded a greater than 90 percent probability of an individual becoming a victim. This trend shows how effective social engineering attacks are continuing to evolve.

Redmon (2005) found that " Odysseus and Sinon used social engineering tactics to get the wooden horse behind the walls of Troy Circa 1671, police officers use social engineering to catch drug dealers, prostitutes, and others criminals; children are often trained to social engineering when they are young, whining or crying as a ploy to get a toy, a bottle or simply attention." If the objective is a genuine or not, the ploys are similar, influence an individual to attain your intended goal.

2.4 Social Engineering in Africa Perspective

This trend has not excluded Africa, with advance fee scam, which rises from various nations in Africa. Herley (2012) found that 51% scam emails originate from Nigeria and additional 34 percent originating from Ghana, Senegal, Burkina Faso, Cote d'Ivoire, and extra West Africa nations. The most famous phishing attack is the Nigerian scam sometimes referred to as "419 scam". Isacenkova, Thonnard, Costin, Balzarotti, and Francillon (2013) have presented a closer look at how 419 Nigerian scam operates and as well as detailed instances of 419 scam operations. It got going by post mail and then developed into a trade conducted via facsimile and later electronic mail. It is a common practice of fraud where assailant deceits victims to pay a definite sum of cash in assurance of a bigger payoff (Isacenkova et al., 2013).

Kenya has induced a fair percentage of attacks originating from social engineering. In 2015 in Garissa, IFMIS passwords of a senior county staffs were stolen and used to make illegal payments, under the Ministry of Devolution, stole credentials were used to access the system and approve fraudulent tender requests and in December 2014 there was a phishing attack in over 5,000 Facebook users (Kigen et al., 2015). Time to time, many mobile users in Kenya receive texts and calls from persons purporting to have sent money wrongfully to their number and hence demanding it back or purporting to have earlier agreed to send the attacker some amount of money but seem to have forgotten the deal. Many M-pesa shop operators and customer have fallen prey to this attack. Several people have complained of being fleeced while conducting online purchases using OLX.

2.5 Social Engineering Threats in eCommerce Platforms

eCommerce and e-business need to safeguard their customers and businesses against numerous forms of social engineering threats. The objective of assaults can vary as attackers may try to exploit their systems using many possible ways. The following are different ways in which attacks can be executed;

i. **Phishing/Spear phishing:** This is a credential harvesting attack. (Brar, Sharma, & Khurmi, 2012) found "an attacker sets up a copy of website they want to impersonate on a remote server." The attacker then replicates the entire website, including its original code, and sends emails to a large number of unsuspecting targets, the emails containing messages that are convincing which will lure the recipient into visiting the spoofed website and revealing his log on credentials. R.Strozer et al. (2014) found "

the phisher sends an email appearing to come from a legitimate business or individual, for example, banks, credit company, or fellow employee, requesting verification of information and warning of dire consequences if it is not provided." Hadnagy and Fincher (2014) termed " Phishing as the practice of sending e-mails that appear to be from reputable sources with the goal of influencing or gaining personal information."

ii. **Baiting/Trojan horse:** An attack which utilizes malware to poison then propagate a bout. Looking authentic, Trojan horse banks on on the inquisitiveness of the prey to click and aiding installation of malware. Interpol (2015) found that sometimes attackers leave an infected storage device to be picked and plugged into a computer by unsuspecting users which intern poisons the system with the malware.

iii. **Pretexting/Reverse social engineering:** An attack that makes and uses a genuine or a designed situation (the pretext) to expand the shot that a focused on casualty will disclose data or perform activities that would be improbable in common conditions (R.Strozer et al., 2014). Ivaturi (2014) found " pretexting as the practice of obtaining information under false pretense, which is often more than a simple lie as it involves a lot of research on the victim before carrying out the attack."

iv. **Social media/ Fraudulent websites:** An attack that uses social media sites such as Facebook and other fraudulent websites into misleading the casualty into tapping on a connection that downloads malware to the casualty's PC

v. **SMSishing:** This attack is similar execution to phishing. The main different is that the fraudulent message is sent via SMS instead of an email in phishing, and targets victims cellular device (Ivaturi, 2014).

vi. **Search engine poisoning:** This attack happens when the assailant tricks people to his website by appealing dishonorable methods. At the point when a simple client taps on the web index comes about, in light of the fact that he trusts it to be pertinent to his question, he is diverted to another site that tries to induce her to download a specific malware unknowingly.

vii. **Diversion theft**- Redirecting a courier or transport delivery to another location (Interpol, 2015)

2.6 Social Engineering Frameworks

2.6.1 Social Engineering Personality Framework (SEPF)

Social engineering personality framework (SEPF) by Uebelacker and Quiel (2014) which is based on relationship between personality traits of the Five Factor Model (Conscientiousness,

extraversion, agreeable, openness and neuroticism) and the six principles of influence (authority, commitment& consistency, reciprocity, liking, social proof and scarcity) used by social engineers. SEPF shows that specific personality traits (According to FFM) of a victim increase or lessen the susceptibility to Cialdini's (2009) principles of influence which are utilized to attack by an attacker, this is portrayed in the framework by use of solid communication channel to represent increase and dashed line to indicate a diminution. General identity presumptions about helplessness (higher, lower or both) for every quality are delineated by relating bolts. This can be stated in Figure 1 below.

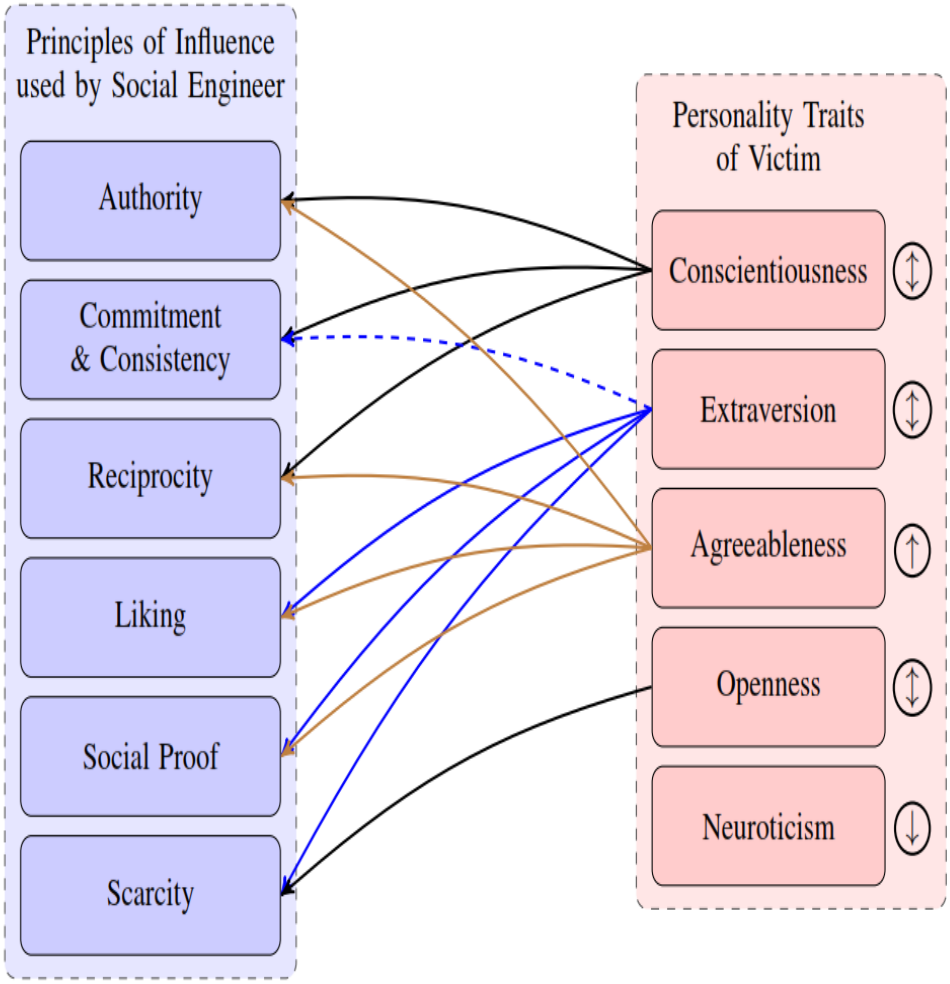

Figure 1: Social Engineering Personality Framework (SEPF) [Source: Uebelacker & Quiel(2014)]

Upon reviewing this framework, the researcher found that it does not quite fulfill the research objective, as the framework only focuses on personality traits and the six factors of influence, omitting the mitigation process.

2.6.2 Social Driven Vulnerability Assessment Framework (SDVAs)

Social-driven vulnerability Assessment framework (SDVAs) create by Frumento and Puricelli (2014) is a crucial element of holistic social engineering risk management, which actively uses SE 2.0 techniques to stimulate an attack against enterprises. The most important components of an SDVA are 1. Realistically simulating the SE based attacks; 2. Assessing the technology-enabled breaks opened as an upshot of the SE based vulnerability; 3. Ethically respecting the employee and comply with the existing legislations; 4. Contextualizing the attacks at either enterprise, team or individual employee levels; 5. Involve the strictly required departments, with the only required details; 6. Analyse and interpret findings correctly, in a deliberative procedure to get a report of results; 7. Apply the answers to find long-term lasting results. From the above elements, they came up with a five-phase framework as shown in figure 3 below. The phase can be briefly explained as follows:

1. Setup Phase: The aim of this stage is to involve only the strictly required stakeholders, explain the threat, share the objectives, limit the scope of the judgment, obtain agreements and retrieve the required data.
2. Passive Social Information Mining phase: Which involves simulating an attacker looking for information about the employees of a company, published mainly on social media in order to advance knowledge of potential victims for making an efficient approach.
3. Spear phishing attack simulation phase: With the core of SDVA is to prove the personal behaviour of an organization against customized hook, which attempts to trick the user to execute an activity that could place at risk the company's assets, possible hooks are biting, tailgating, but the most requested is contextualizing phishing using driven-by-infection or driven by download. The e-mail is properly drafted and contains links to a controlled website that asks to insert a critical information, typically enterprise credentials.
4. Technological attack simulation phase: this phase simulates an attack by making a custom ad-hoc malicious programs from the data phished in phase 2 and 3 respectively on a specific isolated installation, cloned from the enterprise set up for the victim's profiles identified in stage 3.
5. Awareness phase: this phase usually provides training programs to their employees about social engineering.

Figure 2:Social Driven Vulnerability Assessment Framework[Source: Frumento & Puricelli (2014)]

The above-reviewed framework has a strong focus in phishing attack mostly, living out other aspects of social engineering, this then dealigned it with the objectives of the research.

2.6.3 Social Engineering Defensive Framework (SEDF)

Social engineering defensive framework (SEDF) was devised by Valarie Thomas(Gardner & Thomas, 2014b), which was made to offer organizations some assistance with preventing social engineering assaults at the undertaking level. SEDF diagrams four essential stages for assault counteractive action. The phases are autonomous from one another and can be performed in a request that suits the need of the organization, for instance on the off chance that you have finished a substantial training effort, then maybe evaluating defense is the following step. The phases of social Engineering Defensive Framework (SEDF) are 1. Determining exposure- this phase focuses on seeing sites and other available resources as the attacker. 2. Evaluating defenses- this phase can be used to evaluate employee resistance and reaction to simulated attacks. 3. Educate employees-this phase involves teaching employees how attacks are executed and their impacts. 4. Streamlining existing technology and policy-This is through improving effective defensive technologies which are likely in your environment.

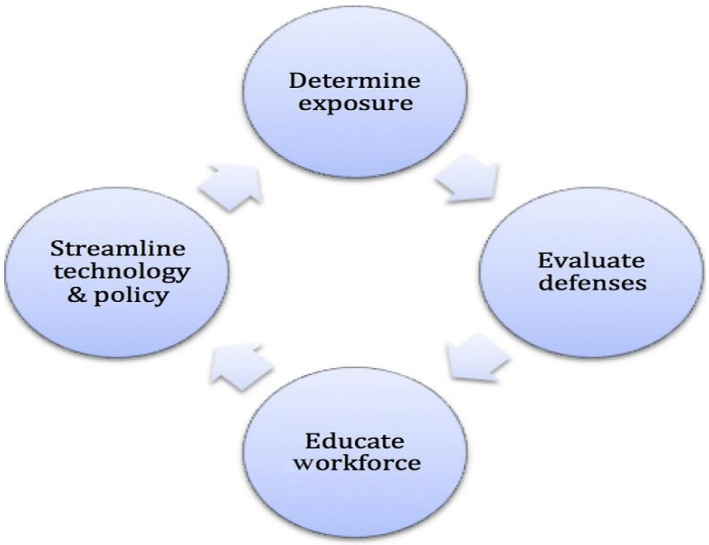

Figure 3:Social Engineering Defensive Framework [Source: Valerie Thomas (2014)]

2.7 Conceptual Framework

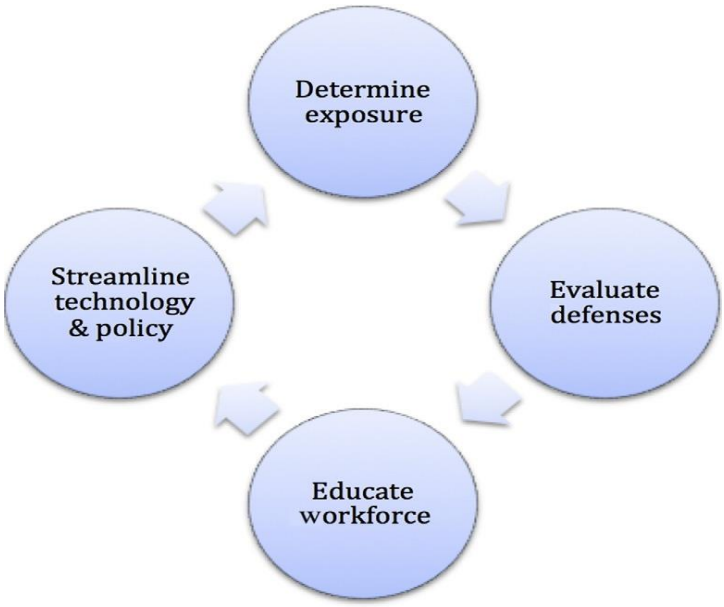

Figure 4: Conceptual Framework (Valarie Thomas, 2014)

Upon the examination of the above frameworks and relating to the problem statement, the researcher adopted Social Engineering Defensive Framework (SEDF) by Uebelacker and Quiel (2014) as it meets all the objectives of the study as shown in Figure 4 below.

Determining exposures, this phase focuses on seeing sites and other available resources as the attacker. Businesses need to take a web exposure assessment, which is a nonintrusive method of gathering client data in order to offer a readable delineation of what data are revealed to the net or leaked information.

Evaluating defenses- this phase was used to evaluate employee resistance and reaction to simulated attacks, evaluate the effectiveness of detection technology and appropriate response groups.

Educate employees-this phase involves teaching employees how attacks are executed and their impacts. Breaking down attack scenarios is essential in social engineering education, as depicting how each bit of information is obtained and how it was employed in the attack builds a genuine discernment of the procedure.

Streamlining existing technology and policy- This is through improving effective defensive technologies which are likely in your environment by improving configuration changes, use new technologies which have provided patches to identified vulnerabilities and creating policies to guide in case employees face social engineering threats.

2.8 Operationalization of Variables

Table 2:Operationalization of Variables

Construct	**Indicators**	**Metrics**
Determine Exposure	I. Providing too much customer data /Data Exposure II. Leaking Sensitive Data Online, in forums, documents or P2P III. Listed in Hacking Sites	• Real life simulation for SE attacks • Hacking sites listing • PII in the internet • PII outside approved physical areas
Evaluate Defences	I. Downloads of documents from phished website & untrusted sources II. Effectiveness of detection technology III. Can Unauthorized person easily access organizations premises IV. Policies and Procedures for information security & different security functions V. Proper discarding of Sensitive data	• How PII is documented & Kept safe • SE risk assessment and evaluation of the organization and contractor • Who can access PII • Separation of obligations to authorize respectability of security checks • Encryption of PII • Data Destruction policies and review frequency • Mitigation controls
Educate Workforce	I. Educating how attacks work, with information from previous	• Mandatory SE and information security Training

	assessment and Emphasis the importance of emails II. Including computer based training (Real simulation of attacks), how to spot social engineering attacks III. Host information sessions on identity theft prevention tips. IV. Using social media safely.	• Communication and posting SE policies • Clear & accessible SE complaints and privacy incident reporting. • Computer based training.
Streamline Technology &Policy	I. Effective defense technologies already existing in the organization's environment II. Social engineering policies in place	• Automatic tools for detecting attacks i.e. IDS, IPS, next-generation firewalls • Data loss prevention • policy violations • Policy updating

Table 3: Operationalization of Variables

CHAPTER THREE
RESEARCH METHODOLOGY

3.1 Overview

This chapter presents the methodology used in this study. The research design, target population, sample size, sampling technique, data collection and data analysis has been outlined.

3.2 Research Philosophy

According to Lewis et al., (2007), research philosophy is the overarching term which identifies with the advancement of information and the way of that learning. It contains an essential suspicion about the path in which you see your reality. This research study was based on Pragmatism research philosophy, which contends that the most critical determinant of the research philosophy used is the examination address one approach might be 'better 'than the other for noting specific inquiries . Johnson and Onwuegbuzie (2004) found that pragmatic philosophy helps to shed a light on how research approaches can be mixed fruitfully, in a way that offers the best opportunities for answering important research questions.

3.3 Research Design

A pre-study of key eCommerce business was used to come up with a list which enables the researcher to identify organizations that are conducting online business. The researcher used the following characteristics to select the eCommerce businesses: Pure-play (Click only) eCommerce firm that still uses physical logistics that assist in delivering systems, owns an interactive website, uses either of the following eCommerce business models, B2B eCommerce, B2C eCommerce or C2C eCommerce and officially residing in Nairobi County(Kabuba, 2012; Schultz, 2009).

This academic study was based on mixed methods mainly quantitative research, which was conducted using the descriptive survey method and qualitative part of the research using content analysis.

3.4 Population and Sample

The objective populace for this study includes eCommerce organizations with official premises in Nairobi County. Gathering accurate information on internet activities especially online trading is exceptionally hard in most developing countries, and Kenya is no exception

(Kabuba, 2012; Souter & Kerrets-Makau, 2012). Nevertheless, the researcher was able to gather insightful information on some of these companies and their range of activities, mostly from online sources like Alexa.com; KBO (Kenya Businesses Online, a Google initiative), Mainstream media (newspapers and media houses, technology blogs (TechMoran), Industry referrals, Information security conferences(africahackon)and a few other authors.

In this academic study, a purposive sample was conducted by utilizing expert knowledge on eCommerce businesses in the Nairobi County to select in a non-random manner sample of commercial enterprises. The aggregate sample constituted to 30 respondents as follows: Jumia.co.ke, Rupu.co.ke, Olx.co.ke, BidorBuy.co.ke, Pigiame.co.ke, Limudi.co.ke, Kaymu.co.ke, MamaMikes.co.ke, Hellofood.co.ke, Killmall.co.ke, Property.n.soko.com, Cheki.co.ke, Jovago.com, Property24.co.ke, Biashara.co.ke, BuyandSell.co.ke, KilaKitu.co.ke, Mpeya.co.ke Mamamealsonwheels.co.ke, Travelstart.co.ke, Eatout.co.ke, Bj's.co.ke, EasyTaxi.com, TicketSasa.com, Pesapal.com, Epepea.com, Emanamba.com, Kopokopo.com, 254Events.com and sleepout.com. The target respondents were IT or Business managers.

3.5 Data Collection

This study collected primary data using questionnaires which comprised of both close-ended and open-end questions. This was considered an effective data collection mechanism particularly in quantitative analysis as respondents would be subjected to the same set of questions. The method is quicker, cost-effective and eliminates researcher's bias and convenient to the respondent as it allows for flexibility.

Questionnaires were developed based on the objectives of the study, both were scrutinized by a senior researcher who critiqued the contents, design, and validity, then guided and corrected accordingly were an issue raised. The documents were passed to two or more Ph.D. candidates for verification and scrutiny. The process was repeated twice for all participants before being administered to the respondents to ensure redundancy-free data would be collected. After the cleansing, the questionnaire would be tested on three different eCommerce organizations. An introductory letter was prepared which accompanied the questionnaire, which gave authenticity to the research and explains the purpose of the study.

3.6 Data Analysis

The gathered data was first checked for consistency and completeness and if correctly filled then weighed to ascertain if it was fit for analysis. In the study, the researcher used descriptive statistics such as mode, frequency counts, percentages and results shown in tables and charts where applicable, to describe the study parameters. In order to establish the relationships among the study variables, inferential statistics will be applied and in testing of the hypotheses.

CHAPTER FOUR

DATA ANALYSIS, RESULTS, AND DISCUSSIONS

4.1 Overview

This chapter presents the data analysis, results, and discussion of the study findings. The findings are presented according to the described methodology, the conceptual framework and the study objectives such that the research questions are answered. The results in this section are from the analysis of data collected. 30 questionnaires were distributed targeting either the IT managers or business manager, with emphasis on IT managers as they most likely to be involved or knowledgeable in the area of study.

4.2 Response Rate

From the questionnaires distributed to the IT managers and Business managers of the online businesses, 24 of them were filled and returned. This translated to 80% response rate, which the researcher considered appropriate to facilitate in making conclusions and recommendations. The remaining 20% did not react to the questionnaires, as they perceived the research topic to be sensitive in nature, particularly the section requesting for evaluating social engineering threats. A conglomerate of six eCommerce businesses did not react to the questionnaire as they perceived the research topic to be against their company data exposure policy.

4.3 Demographics

To capture general information, the researcher sought to establish the age of the organizations, ownership, the position of the respondents and the education level of the respondents. The table 5 under illustrates the finds, which shown that 70.8% are in existence in less than 5 years, 25% are in operation between the ages of 6-10 years and 4.2% have made between the ages of 11-15%.

Table 4:Organisation's Age

Organization's Age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0-5 Years	17	70.8	70.8	70.8
	6-10 Years	6	25.0	25.0	95.8
	11-15 Years	1	4.2	4.2	100.0
	Total	24	100.0	100.0	

Further analysis showed that more than 50% are locally owned eCommerce organizations, then followed by 29.2% of foreign owned and lastly 20.8% eCommerce systems are both Locally and Foreign owned. The results are illustrated in table 5 below:

Table 5: Categorization of the organization owning

Categorization of the organization owning

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Locally Owned	12	50.0	50.0	50.0
	Foreign Owned	7	29.2	29.2	79.2
	Combination of Locally and Foreign	5	20.8	20.8	100.0
	Total	24	100.0	100.0	

The target respondents in targeted organizations were IT and Business managers, but with the emphasis, more on IT managers as they were perceived to have a deeper understanding of the research subject. This was exemplified in table 6 below which show that 87.5% of the respondents were IT managers and 12.5% are Business managers.

Table 6:Job position of the respondents

Job position of the Respondent

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Business Manager	3	12.5	12.5	12.5
	IT Manager	21	87.5	87.5	100.0
	Total	24	100.0	100.0	

The researcher sought to establish the education level of the respondents. The analysis demonstrated that respondents with postgraduate studies recorded the highest percentage of 54.2%, This mostly covered those who had mastered. The remaining 45.8% represents those

who are University graduates, holding a degree. The higher number of graduate students and master's holders indicates a serious chance of receiving a high grade of character data. This is instanced by the table 7.

Table 7:Education of the respondents

Highest degree of education achieved

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	University Graduate	11	45.8	45.8	45.8
	Postgraduate	13	54.2	54.2	100.0
	Total	24	100.0	100.0	

4.4 Social Engineering Threats

The researcher sought to establish social engineering threats that eCommerce businesses in the country are facing with the view to compare what has already been indicated from previous empirical studies. The respondents were asked to tell whether they face those threats in running their day-to-day actions. This is instanced in the table beneath. From table 8, it shows that Phishing is the biggest threat as most eCommerce businesses have faced the menace. This is indicated by 30.4% in percent of responses and 100% in percent of cases which were taped. Baiting/Trojan horse and Social Media/Fraudulent websites had equal shares of 25.2 percent of responses and 50% of the cases recorded. SMSishing and Diversion Theft had an equal share of 7.6% percent of responses and 25% of the events note. Pretext/Reverse social engineering had 11.4% percent of responses and 37.5% of the cases noted, followed lastly by Search Engine poisoning which a case of 12.7% percent of responses and 41.7% of the cases recorded. This was attributed to the uniqueness of the attack and that those who were using the search engine without knowledge of how the attack is perpetrated, they fall victim easily. For instance, some respondents agree to have severally been redirected to a search engine similar to Google Search, which was not legitimate.

Table 8:Social Engineering Threats

Social Engineering Threats Frequencies				
		Responses		Percent of Cases
		N	Percent	
Social Engineering Threats	Phishing/Spear phishing (e-mails that appear to be from reputable with intent to gaining access to personal information)	24	30.40%	100.00%
	Baiting/Trojan Horse (victim to click and aid installation of malware on the targeted computer)	12	15.20%	50.00%
	Pretexting/Reverse social Engineering (Obtaining goods by false pretense)	9	11.40%	37.50%
	Social Media/Fraudulent website	12	15.20%	50.00%
	SMSishing	6	7.60%	25.00%
	Search Engine poisoning	10	12.70%	41.70%
	Diversion Theft	6	7.60%	25.00%
Total		79	100.00%	329.20%
a. Dichotomy group tabulated at value 1.				

The researcher conducted a controlled phishing exercise to the target respondents, where to spear phishing emails were sent to the target organizations, which were not attached to any infectious payload or rootkit, but with a reverse TCP shell which would spawn a command shell on a victim and send back using the Social Engineering Tool Kit (SET). Figures 5, 6, 7, 8, 9 and 10 below shows the setup of the spear phishing simulation phase from Social Engineering toolkit(SET).

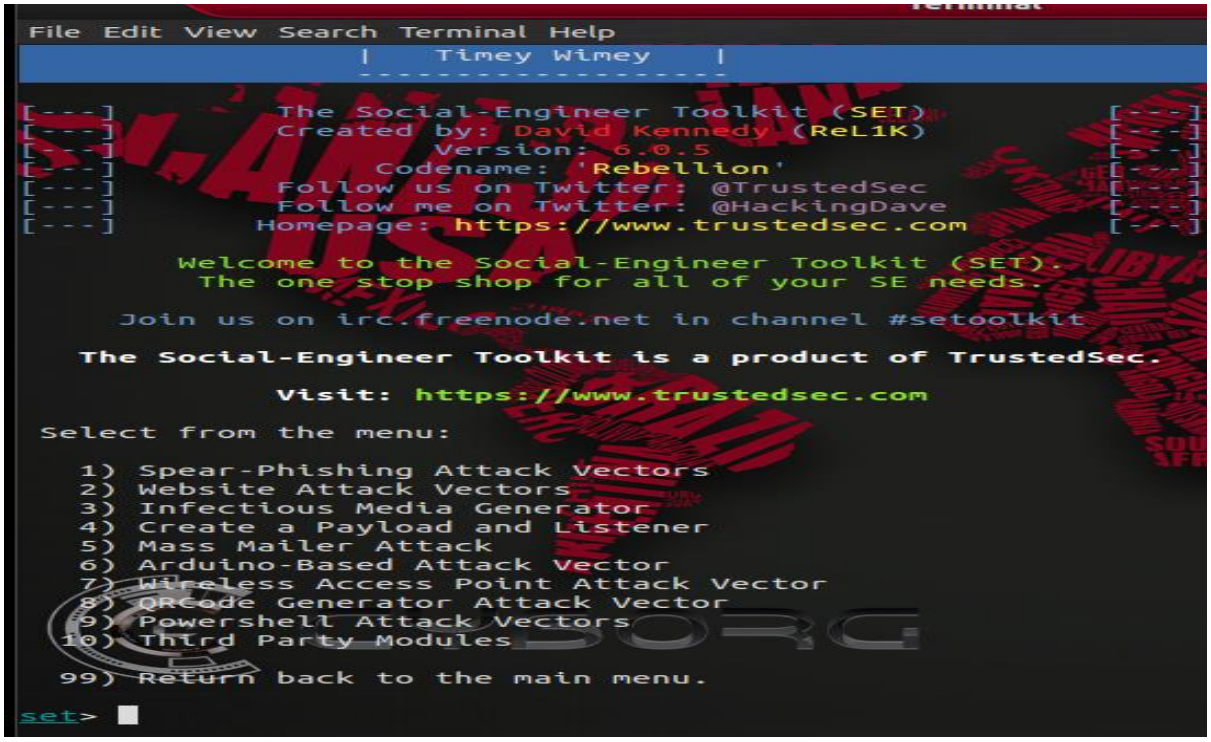

Figure 5: Spear Phishing Simulation step one

This was followed by selecting the selecting of the file format exploit where the research chose to use option four cause it's easy for unsuspecting users to download word document due to widely use of windows products. This created a Word document with a buffer overflow and enabled including a listener to target victim machine.

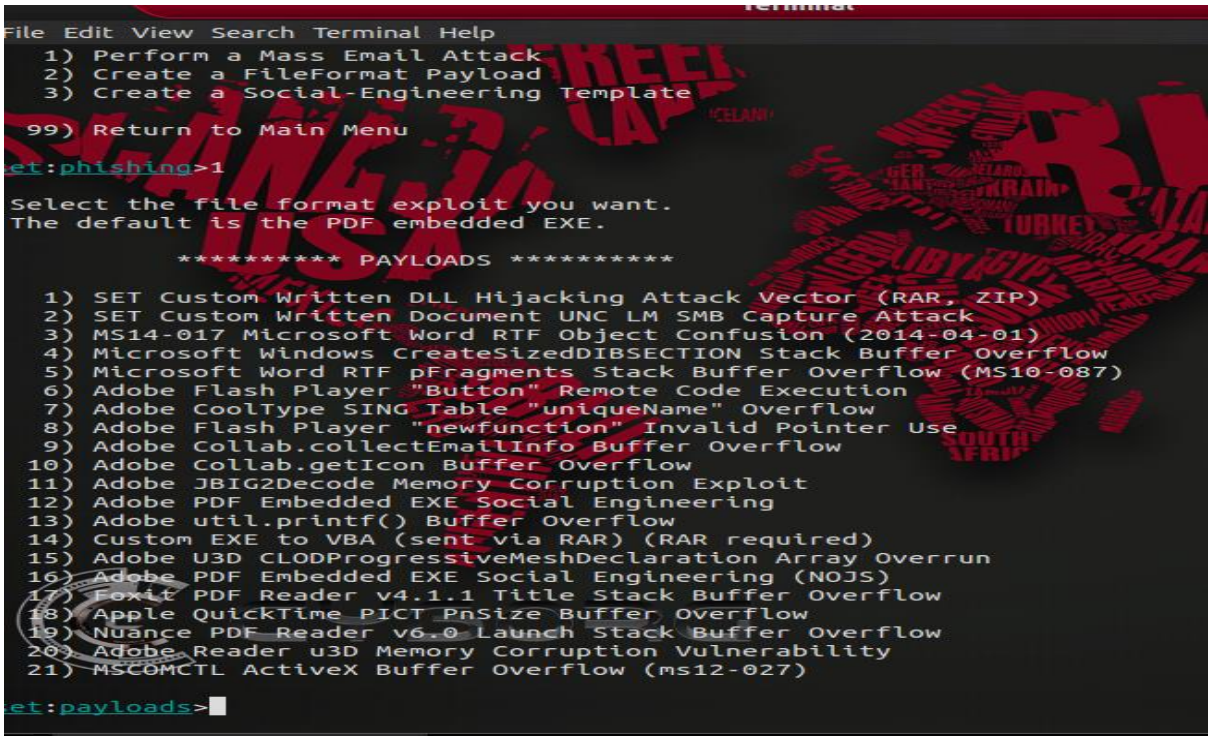

Figure 6: File Format selection

After deciding on which type of file to use in the attack, the next step was to choose which type of listener or payload to dump in the victims' machine as shown in the figure below.

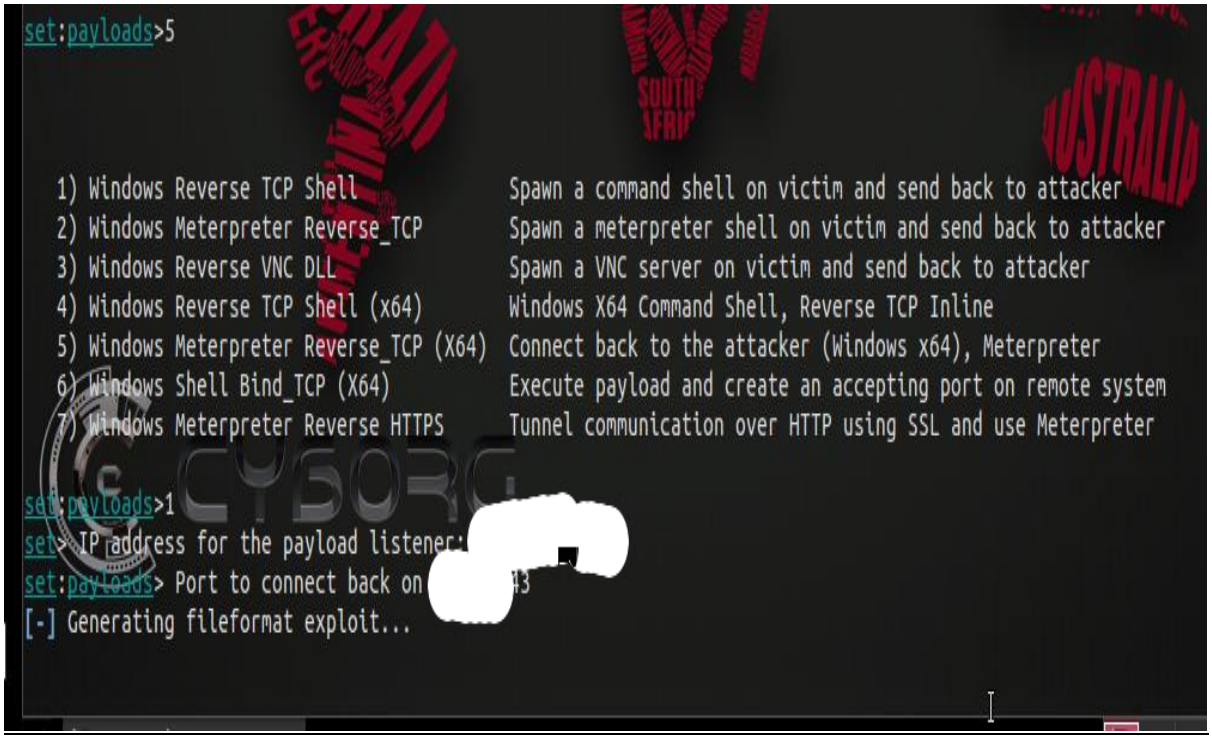

Figure 7: Choosing listener or Payload

Creating the malicious file name and renaming proceeded as illustrated

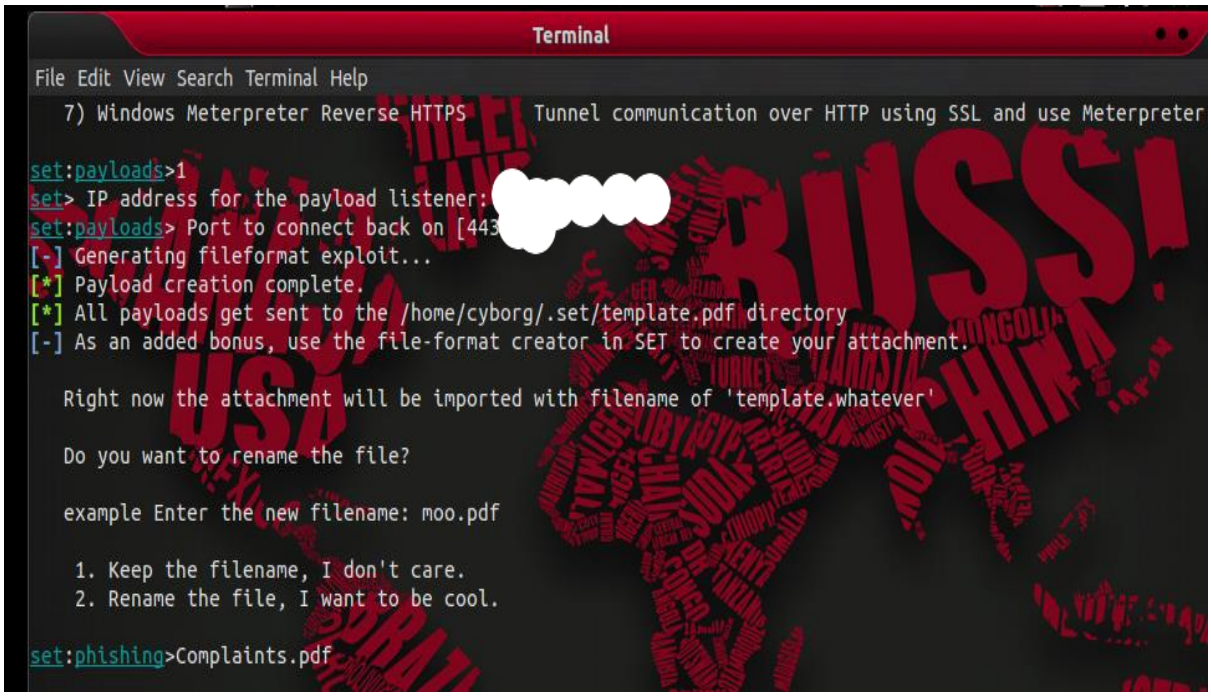

Figure 8:Naming the attack file

The second last step was crafting the email. Since most eCommerce organizations, just as any other business entity focus on high sales which translate to high turnover and in turn increase ROI. The researcher crafted an email to the target organizations as shown below.

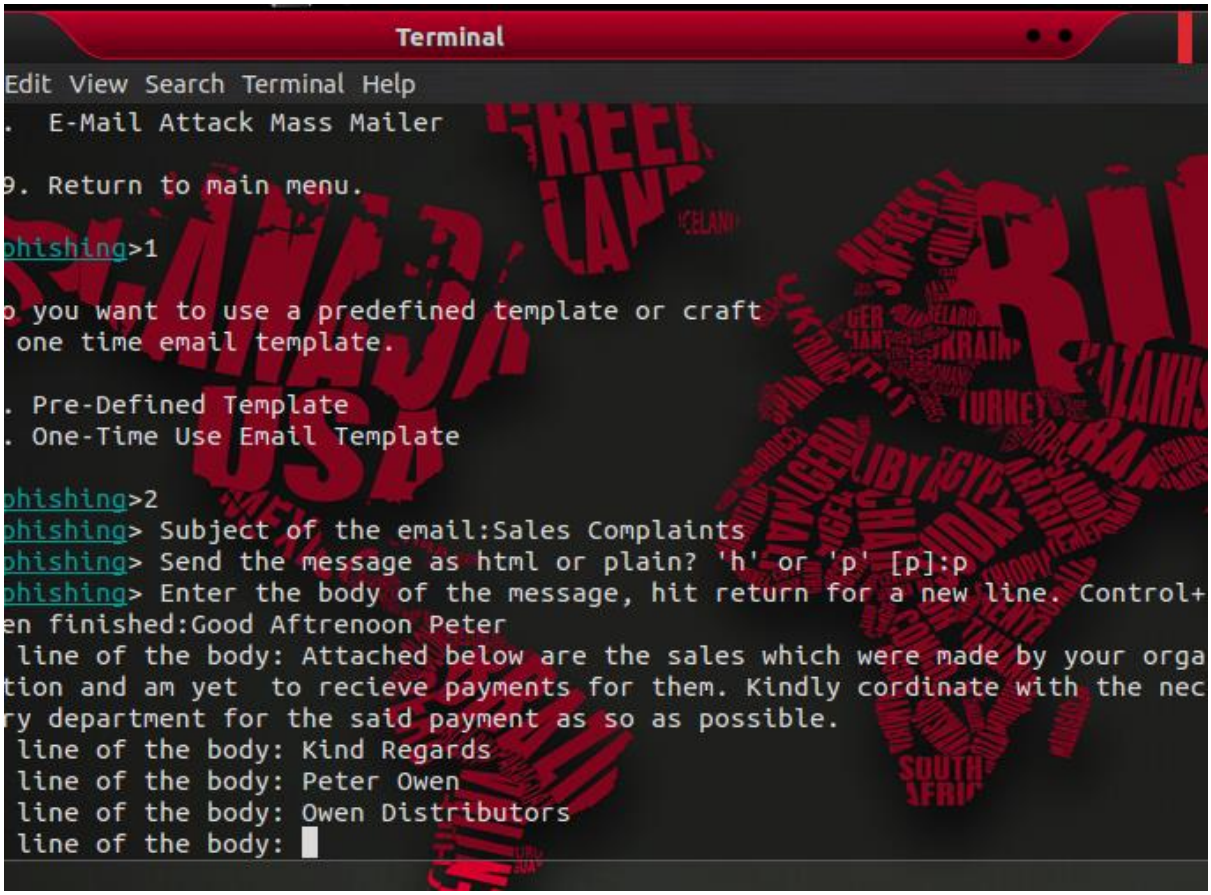

Figure 9:Crafting email

After that, the SET prompted to whether use Gmail or SMPT email account. From there, the researcher chooses an appropriate method and received all the notification of the spear phishing email in the chosen account as shown below

Figure 10: Choosing Account

From the controlled environment, it was confirmed that phishing is a big menace in online companies, as most of the organizations fell victim of the spear phished email by clicking it. This is illustrated by the table below, where 95.8% of the target respondent responded to the email by clicking on the Phishing Link and 4.2% did not.

Table 9:Phishing/Spear Phishing simulation

Phishing/Spear Phishing Real Life Simulation Links

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not Clicked	1	4.2	4.2	4.2
	Clicked	23	95.8	95.8	100.0
	Total	24	100.0	100.0	

This re-enforces that many of eCommerce platforms are highly susceptible to social engineering and that they need proper ways to contain the threats. The phishing exercise details that the organizations are vulnerable to other social engineering attacks like Baiting or Trojan horse, where attackers can attach an infectious payload to the phishing email and when it's clicked, the infectious payload will be downloaded to the target machine and from there it can be used to execute the intended purpose.

4.6 Dimensions of Social Engineering Defensive Framework

The results, which test the dimensions of Social Engineering defensive framework, have been summarized in table below

Table 10: Social Engineering Defensive Framework Dimensions (Source: Research Data, 2016)

Statements	**Not at All**	**Small Extent**	**Moderate Extent**	**Great Extent**	**very Great Extent**	**Mode**
	%	%	%	%	%	
Testing and checking privacy and information security controls?	-	-	-	25	75	5
Conducting internet searches to settle and remove data in the public arena	-	4.2	4.2	16.7	75	5
Searching information system and computer storage to distinguish PII outside endorsed ranges?	-	-	-	12.5	87.5	5
Checking organization website listing in hacking forums?	25	25	41.7	8.3	-	3
Document personal data and other sensitive information maintained by your organization	-	-	-	12.5	87.5	5
Social engineering risk assessment and evaluate privacy threats evaluation	-	-	-	12.5	87.5	5
Authorized access to sensitive data and PII	-	-	16.7	33.3	50	5

Job Segregation to ensure integrity of security checks and counterbalances	-	-	20.8	50	29.2	4
Data migration controls	-	-	-	12.5	87.5	5
Security controls, such as encryption	-	-	16.7	37.5	45.8	5
Revising and possession current data destruction policies	-	-	12.5	4.2	83.3	5
Provide mandatory social engineering and data security training, repeatedly to different staffs involved and business partners	-	-	-	33.3	66.7	5
Do you communicate and post social engineering approaches to clienteles and consumers (For delineation, on the association's site, or on a notice board at the workplace, through statements inserted into text files or electronic mails)	-	-	-	20.8	79.2	5
Have you clearly found and made effortlessly open process for reporting protection episodes and dissensions (Contingent upon the direction of the subject, this may incorporate answering to the powers, open and additionally people)	-	-	4.2	8.3	87.5	5
Employ automatic tackles, like Intrusion detection/prevention systems, next generation firewalls, to screen and alert about suspicious or strange movement	-	-	-	12.5	87.5	5
Use information loss prevention which tracks the development and utilization of data inside your organisation and controlling the unexpected disclosure of individual touchy information, for both information at rest or in motion	-	-	-	20.8	79.2	5
Conduct policy violations to determine if they are well utilized?	-	-	-	16.7	83.3	5
Periodically update and document new policies, regarding social Engineering threats noted and documented						

The respondents were required to state to what extent they determine the exposure of sensitive data or personal Identifiable data in their organizations, evaluate defenses of their systems, educate the workforce on social engineering and Streamlining technology and policies. They would then tick appropriately to a Likert scale ranging from 1 – 5, to a very great extent rated at 5, the great extent at 4, moderate extent at 3, small extent rated at 2 or not at all which was rated at 1. The analysis was done in terms of the frequency (F) of respondents in each scenario and mode calculated.

4.6.1 Determining Exposure

Caved in the extremely active growth of Social Engineering attacks, threats, knowledge of what aspects concern organizations are a prerequisite for effectively protecting your organization against social engineering. The researcher sought to establish how eCommerce organizations are strategizing on how they determine the exposure of sensitive data to social engineering attackers. The following elements were considered important: Testing and checking privacy and information security controls, how often do organisations conduct internet searches to settle and remove data in the public arena, searching information system and computer storage to distinguish PII outside endorsed ranges and lastly Checking organization website listing in hacking forums.

Table 10 shows that testing and checking privacy and information security controls had responses which indicate that 75% of the organization do implement, 75% of organizations do conduct internet searches to settle and remove data in the public arena and 87.5% do conduct regular search information system and computer storage to distinguish PII outside endorsed ranges; and they entirely induce a mode 5 from the results submitted. Checking if organizations' websites are listed on hacking websites like kickasspaste.com, pastebin.com, ghostbin.com et cetera, had 41.7%. This indicates that most of the arrangements in question do not concur and think that their organizations' websites can’t be listed on hacking forums. This might be as an upshot of the respondents not knowing if such websites exist or due to negligence and ignorance.

4.6.2 Evaluating Defenses

Evaluating defenses is one key process that which will assist an organization to reflect what is going on and in establishing what is needed in order to seal any security loopholes. The research sought to establish how E - commerce organizations evaluate their information security defenses with the following attributes considered to be important: document personal data and other sensitive information maintained by your organization, where it is stored and how it's held securely, conducting regular social engineering risk assessment and privacy threats evaluation, reviewing who is authorized to access to sensitive data and PII, job segregation to ensure integrity of security checks and counterbalances, implementing data migration controls to detect unapproved contact, stealing or misuse of personal indefinable data & additional profound material, implement security controls, such as encryption of data in motion & at rest and revising and possessing current data destruction policies, to downplay

jeopardy of data through unsanctioned contact to archived media or information processing systems which were formerly used.

From table 10, it shows that documenting personal data and other sensitive data maintained by the system, conducting regular Social engineering risk assessment and job segregation all had 87.5% of the responses filled. Approving whom to access sensitive data and implementation of mitigation and security controls all score 79% of the response case. All the elements had a mode of 5. This shows that the organizations keep on evaluating their security arrangements, policies and processes in parliamentary procedure to keep the up –to –date and hence thwart any attacks to their information systems.

4.6.3 Educating Workforce

Describing an attack can be informative, but showing an attack has a far greater impact (Gardner & Thomas, 2014a). The researcher tried to show how eCommerce organizations are educating their employees, contractors and business partners on social engineering threats. The following elements were considered important: providing mandatory social engineering and data security training, repeatedly to different staffs involved and business partners, communicating and posting social engineering approaches to clienteles and consumers (For delineation, on the association's site, or on a notice board at the workplace, through statements inserted into text files or electronic mails), Have you clearly found and made effortlessly open process for reporting protection episodes and dissensions (Contingent upon the direction of the subject, this may incorporate answering to the powers, open and additionally people).

The most vulnerable link in data security is the end- user. Organizations should make certain that their workforce and business partners are aware of social engineering as it keeps changing with new ploys being created with each fleeting day. The analyzed information in table 10 shown that the sampled organizations all had put emphasis to training their workforce and business partners, this is shown by a frequent mode of 5 in all the three elements and with 83%, 66.7%, and 79.2% percent in responded cases.

4.6.4 Streamlining Technology and Policies

While innovation alone can't avoid social engineering assaults, it can minimize the effect of fruitful ones. Viable cautious advances likely exist in your surroundings, however, could enhance with design modifications. The researcher examine how eCommerce programs are

faring in streamlining their technologies and policies, the following rudiments being considered vital : employ automatic tackles, like Intrusion detection/prevention systems, next generation firewalls, to screen and alert about suspicious or strange movement, use of information loss prevention which tracks the development and utilization of data inside your organisation and controlling the unexpected disclosure of individual touchy information, for both information at rest or in motion, conduct policy violations to determine if they are well utilized and periodically updating and documenting new policies, regarding social engineering threats noted.

Table 10 above indicates that most organizations employ automated tools, like intrusion detection and prevention systems, next generation firewalls wall to monitor and alert about suspicious or anomalous activities having 87.5% together with making easily accessible the process of reporting privacy incidents and all had a mode of 5 of the responded cases. Use information loss prevention which tracks the development and utilization of data inside your organisation and controlling the unexpected disclosure of individual touchy information and conduct policy violations to determine if they are well utilized and periodically updating and documenting new policies, regarding social engineering threats noted all had a mode of 5. This is a positive note and indicates that the organization under investigations are faring well in streamlining technology and policies, but still, they have to work hard on ensuring that they periodically update and document new policies, regarding social Engineering threats noted and documented.

4.7 Hypotheses Testing

The researcher sought to establish if there was a relationship between Educating workforce and social engineering threats. The study was conducted by the following research hypotheses:

4.7.1 H_0: Social engineering training will lead to decreased attacks on eCommerce platforms in Kenya

The test variable for H0: Educating Workforce

Grouping variable: Type of eCommerce

Table 11:Group statistics and Independent sample test

Group Statistics

	Type of eCommerce the firm Uses	N	Mean	Std. Deviation	Std. Error Mean
Educating Workforce	Pure play (Conduct their business online)	22	4.7879	.26318	.05611
	click and mortar (Sell online and have physical premises)	2	4.5000	.70711	.50000

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Educating Workforce	Equal variances assumed	10.524	.004	1.308	22	.204	.28788	.22014	-.16866	.74441
	Equal variances not assumed			.572	1.025	.667	.28788	.50314	-5.74360	6.31936

An Independent-Sample *t*-test was calculated comparing the mean score of Educating workforce to the mean score of eCommerce type. No significant difference was found (t (22) = 1.308, $p > 0.5$). The mean of eCommerce organizations which conduct click and mortar (sell online and have a physical premise) (m = 4.50, SD = 0.707) was not significantly different from the mean of organizations which conduct pure play (m = 4.79, SD = 0.263). Cronk (2012) stated that reject the null hypothesis if the output value under *sig*. (Sometimes *p* or *alpha*) is equal to or smaller than .05 and fail to reject the null hypothesis if the output value is larger than .05. In this case, we accept the null hypotheses as of the $p > 0.05$ and reject the alternative hypothesis H_A.

4.8 Best Practices

According to Parsons et al., (2010), there are several defenses that an organization can use to protect itself against social engineering threats and many of these mechanisms are simple to implement. To effectively defend against social engineering attacks, it is necessary for organizations to have a multifaceted approach (Janczewski & Fu, 2010). Many researchers have classified and grouped social engineering mitigations in different categories, but they all

lead to policy, audit and awareness training (Chaudhry, Chaudhry, & Rittenhouse, 2016; Kumar, Chaudhary, & Kumar, 2015; Papadaki & Furnell, 2009; Redmon, 2005; Spinapolice, 2011). From research data, the researcher came up with best practices which should be utilized by eCommerce organizations to protect themselves from social engineering attacks and threats based on the dimensions the framework used. The requirements and preferred practices are listed below:

i. Understand as an organization, what is safe to broadcast to the web or public and only necessary information should be communicated or availed to the masses and remove any personally identifiable information that is in the public domain.
ii. Email addresses, information of high profile people, clients, business partners and persons of interest in the organizations should be kept secret
iii. Periodically test and check privacy and information protection command
iv. Regularly check if the organization's website is listed in hacking forums like pastebin.com, ghostbin.com or anonpaste.com
v. Document personal data and other sensitive information maintained by your establishment and ensure its stored securely and as per laws and regulations in place
vi. Regularly conduct social engineering risk assessment and evaluate threats to your organization, contractors, and business partners
vii. Ensure physical security to the organization information system and accessing the said systems should be through authorized personnel only. This can be enforced through the use of guards, biometrics, alarm systems and log files.
viii. Implementing data migration controls to detect unapproved contact, stealing or misuse of personal indefinable data & additional profound material
ix. Implementing security controls, such as encryption of data in motion & at rest.
x. Regularly revising and possessing current data destruction policies, to downplay jeopardy of data through unsanctioned contact to archived media or information processing systems which were formerly used.
xi. Providing mandatory social engineering training on a regular base
xii. Communicating and posting social engineering policies to employees, business partners, and customers, on the organization's website, emails and memos on the notice board in the organization
xiii. Making clearly found and effortlessly open process for reporting protection episodes and dissensions

xiv. Using automatic tackles, like intrusion detection/prevention systems, next generation firewalls, to screen and alert about suspicious or strange movement in the organization's network.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.1 Overview

This chapter provides a summary of the research conclusions and recommendations as noted by the researcher. It too levels out the limitations of the written report and provides hints for further inquiry as well as implications of the study of policy and practice.

5.2 Conclusion

This academic research study seeks to investigate social engineering and it's mitigation in eCommerce platforms in Kenya. To accomplish this aim, the researcher looked into three social engineering mitigation frameworks and adopted Social Engine Defensive Framework in developing a conceptual framework.

The analysis of the quantitative data gathered from the duly filled questionnaires and the identification of various issues that arose from qualitative data that was collected through drop & pick questionnaires and online questionnaires has informed the best practices. The analysis covered social engineering threats in eCommerce Platforms in Kenya and mitigation measures using the four dimensions of Social Engineering Defensive Framework namely, determining exposure, evaluating defenses, educating the workforce, streamlining technology & policy and demographic areas like ownership of the eCommerce organization.

The results show that most eCommerce organizations have been affected by social engineering and phishing as the leading social engineering threat with 100% of cases tapped followed by baiting/ Trojan Horse and social media/ fraudulent websites each tying with 50 %. Search engine poisoning, pretext/ reverse social engineering, and diversion, theft had 41.7%, 37.5% and 25% of the events recorded.

Mitigation measures from the four phases of the conceptual framework indicate that in (a) determining exposure's analyzed data indicates the organizations to be faring well, but checking organizations website listing in hacking sites like Pastebin.com., anonghost.com, ghostbin.com et cetera, was least responded. Most organizations did not coincide with their organizations being listed at such websites and forums. This might have been as a result of the respondents not knowing if such sites exist or due to negligence and ignorance. (b) Evaluating defenses: The researched findings showed organizations keep on evaluating their security systems, policies and procedures in a parliamentary procedure to keep them up-to-

date. (c) Educating workforce: the findings indicated that the sampled organizations fared well. Lastly (d) Streamlining technology and policies: the findings indicated a positive note, but still they need to ensure they periodically update and document new policies regarding social engineering and information protection

This research offers best practices derived from the four phases of the social engineering defensive framework and was deemed essential after research analysis.

5.3 Recommendations

The research has led to strategies that would enhance successful mitigation of social engineering attacks and threats and hence it would ensure safe systems for customers, business proprietors, and their stakeholders.

For policy makers and senior level managers, they need to ensure that apart from using the derived best practices, they ought to have the following in their arsenal for mitigating social engineering: Physical security of their business premises, having information security policies and procedure in place, which are up-to-date, securing the whole organization and incorporating security culture in an organization Oosterloo (2008). The ultimate way to tackle social engineering is through creating awareness, this involves teaching and including desktop simulation of social engineering attacks and ensuring that social engineering mitigation tactics need to be updated time after time due to the evolving nature of social engineering by the creativity of the attacker.

For individuals protect themselves from social engineering, they should observe: not clicking on embedded email links and download attachments from unknown senders, Patch software's and operating schemes, use up to date antivirus software, pay attention to URLs and ensure are secured with Https before sending sensitive info, never provide personal info unless you're sure to do so, and lastly be weary of unknown phone calls and SMS asking for your personal data or employee information.

5.4 Limitation of the study

The inquiry was limited to eCommerce business that holds permanent residence in Nairobi locality, excepting those which are residing outside the County. Most eCommerce organizations hold no official documentation or records which can be utilized by researchers Kabuba (2012).

eCommerce sector in Kenya is still in the formative stages, a majority of the companies are nevertheless in the start-up stage, there was great tendency for these societies to be reluctant and overprotective in divulging sensitive information as they perceived the research topic to be sensitive in nature, especially the section requesting for evaluation of social engineering threats and felt may leak to competitors. Most of these societies are keen to retain and protect any valuable resource that may yield them a competitive edge in the marketplace. This, of course, made it hard to get the needed information. Some questionnaires had unanswered questions which made it difficult to examine data in some offices. This can cause non-response biased, which can affect the validity and reliability of the outcomes, though not to a large extent

5.5 Further Research

Further research should be carried out to establish if social engineering affects differently in different cultures and regions and to what extent? Evaluate and establish apart from principles of influence and personality traits, can attitude and ignorance influence susceptibility to social technology.

Further research should be carried out to assess terrorism, cyber warfare, and social engineering in East African countries and its countermeasures and a recommendation of new methods to mitigate social engineering.

REFERENCES

1. Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society, 32*(3), 183-196.
2. Brar, T. P. S., Sharma, D., & Khurmi, S. S. (2012). Vulnerabilities in E-banking: A Study of Various Security Aspects in E-banking. *International Journal of Computing & Business Research*.
3. CAK. (2015). *First Quater Sector Statistics Report for the Financial Year 2016/2016*. Retrieved from
4. Cert-UK. (2015). Introduction-to-social-engineering., 1-10. Retrieved from WWW.cert.gov.uk website:
5. Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016). Phishing Attacks and Defenses. *International Journal of Security and Its Applications, 10*(1), 247-256.
6. Cialdini, R. B. (2009). *Influence The Psychology of Persuation*
7. Cronk, B. C. (2012). *How to use SPSS statistics: A step-by-step guide to analysis and interpretation*: Pyrczak Pub.
8. FBI. (2015). *Business Email Compromise*. Retrieved from http://www.ic3.gov/media/2015/150827-1.aspx
9. Frumento, E., & Puricelli, R. (2014). An Innovative and Comprehensive Framework for Social Vulnerability Assessment. *Magdeburger Journal Zur Sicherheitsforschung, 2*, 493-505.
10. Gardner, B., & Thomas, V. (2014a). *Building an information security awareness program : defending against social engineering and technical threats*. Amsterdam ; Boston: Elsevier/Syngress.
11. Gardner, B., & Thomas, V. (2014b). *Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats*: Elsevier.
12. Hadnagy, C., & Fincher, M. (2014). *Phishing Dark Water: The Offensive and Defensive Sedes of Malicious E-mails* (2 ed.). Indianapolis, Indiana: John Wiley & Sons
13. Hasan, M., & Harris, E. (2009). Entrepreneurship and Innovation in eCommerce. *Journal of Achievements in Materials and Manufacturing Engineering, 32*(1), 92-97.
14. Herley, C. (2012). *Why do Nigerian scammers say they are from Nigeria?* Paper presented at the WEIS.

15. Interpol. (2015). Social Engineering Fraud. Retrieved from http://www.interpol.int/fr/Crime-areas/Financial-crime/Social-engineering-fraud/Types-of-social-engineering-fraud
16. Isacenkova, J., Thonnard, O., Costin, A., Balzarotti, D., & Francillon, A. (2013). *Inside the Scam Jungle: A Closer Look at 419 Scam Email Operations.* Paper presented at the IEEE Security and Privacy Workshop.
17. Ivaturi, K. R. (2014). *Social Engineering - Emerging Attacks, Awareness and Impact on Online User Attitudes and Behaviour.* (Doctor of Philosophy), University of Auckland, University of Auckland Research Repository - ResearchSpace.
18. Janczewski, L. J., & Fu, L. (2010). *Social engineering-based attacks: Model and new zealand perspective.* Paper presented at the Computer Science and Information Technology (IMCSIT), Proceedings of the 2010 International Multiconference on.
19. Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. *Educational researcher, 33*(7), 14-26.
20. Kabuba, P. K. (2012). *eCommerce and Performance of Online Businesses in Kenya.* Univeristy Of Nairobi, Nairobi. (1-62)
21. Kigen, P. M., Kimani, C., Mwangi, M., Shiyayo, B., Ndegwa, D., Kaimba, B., & Shitanda, S. (2015). *Kenya Cyber Security Report 2015*. Retrieved from Nairobi:
22. Kinuthia, J. N. K., & Akinnusi, D. M. (2014). The Magnitude of Barries Facing eCommerce Businesses in Kenya. *Journal of Internet and Information Systems, 4*(1), 12-27.
23. Koteswara, I., & Janczewski, L. (2014). Social Engineering Preparedness of Online Banks: An Asia-Pacific Perspective. *Journal of Global Information Technology Management, 16*(4), 21-46. doi:10.1080/1097198x.2013.10845647
24. Kumar, A., Chaudhary, M., & Kumar, N. (2015). Social Engineering Threats and Awareness: A Survey. *European Journal of Advances in Engineering and Technology, 2*(11), 15-19.
25. Lewis, P., Thornhill, A., & Saunders, M. (2007). *Research methods for business students*: Pearson Education UK.
26. Luo, X. R., Brody, R., Seazzu, A., & Burd, S. (2011). Social Engineering: The Neglected Human Factor for Information Security Management. *Information Resources Management Journal, 24*(3), 1-8.
27. Mirescu, S. V. (2011). The Premises and Evolution of Electronic Commerce. *Journal of Knowledge Management, Economics and Information Technology, 1*(1), 1-12.

28. Mulwa, D. K. (2012). *A survey of insider information security threats management in commercial Banks in Kenya.* University of Nairobi.
29. Mutuku, M. K., & Kyalo, J. K. (2015). Determinants of Profitability of eCommerce Operations in the Communication Sector in Nairobi County, Kenya. *International Journal of Education and Research, 3*(3), 1-14.
30. Oosterloo, B. (2008). *Managing Social Engineering Risk: Making social engineering transparent.* University of Twente.
31. Papadaki, M., & Furnell, S. (2009). Social engineering: assessing vulnerabilities in practice. *Information Management & Computer Security, 17*(1), 53-63.
32. Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010). Human factors and information security: individual, culture and security environment.
33. ProofPoint. (2016). *The human factor report 2016*. Retrieved from https://www.proofpoint.com/us/human-factor-report-2016
34. R.Strozer, J., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2014). Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits. *2014 IEEE Security and Privacy Workshop*.
35. Redmon, K. C. (2005, November 29). *Mitigation of Social Engineering Attacks in Corporate America*. Greenville.
36. Schultz, P. (2009). *Behind the Internet Business Models: An E-health Industry Case*. Masters Thesis. Copenhagen Business School.
37. Souter, D., & Kerrets-Makau, M. (2012). *Internet Governance in Kenya- An Assessment for the Internet Society*. Retrieved from
38. Spinapolice, M. (2011). Mitigating the risk of social engineering attacks.
39. Team, V. R. (2015). 2015 Data Breach Investigations Report.
40. Torres, A. (2014). *Social Engineering*. Retrieved from http://www.securingthehuman.org
41. Uebelacker, S., & Quiel, S. (2014). *The Social Engineering Personality Framework.* Paper presented at the 4th Workshop on Socio-Technical Aspects in Security and Trust (STAST), , Vienna, Austria.
42. Victoria, A. (2013). *eCommerce Adoption Among Small And Micro Enterprises in Nairobi.* UON.
43. WTO. (2013). *Opportunities and Challenges for Small and Medium-Sized Enterprise*. Retrieved from

APPENDICES

APPENDIX I: Introduction Letter

UNIVERSITY OF NAIROBI

COLLEGE OF BIOLOGICAL AND PHYSICAL SCIENCES SCHOOL OF COMPUTING AND INFORMATICS

Telephone: 4447870/4444919/4446544
Telefax: 4447870
Email: moturi@uonbi.ac.ke

P. O. Box 30197
00100, GPO, Nairobi
Kenya

24 May 2016

TO WHOM IT MAY CONCERN

LAWRENCE MWAGOTI MWASAMBO (P54/73325/2014)

The above named is a student in the MSc in Information Technology Management of the University of Nairobi. As part of the requirements of the programme, the student is required to undertake a research project and write a report. His project is entitled: **Social Engineering in eCommerce Platforms in Kenya.**

I am therefore requesting that you assist the student to obtain the required information. Your assistance will be highly appreciated.

Yours faithfully,

CHRISTOPHER A. MOTURI DEPUTY DIRECTOR

SCHOOL OF COMPUTING AND INFORMATICS

APPENDIX II: Personal Introductory letter

Date…….

Business Manager

……

P.O Box …….

Nairobi.

Dear Sir,

RE: ACADEMIC RESEARCH PROJECT

I' am a Masters student at the University of Nairobi. I wish to conduct a research entitled "**SOCIAL ENGINEERING IN E- COMMERCE PLATFORMS IN KENYA**". A questionnaire has been designed and will be used to gather relevant information to address the research objectives of the study. The purpose of writing to you is to kindly request you to grant me permission to collect information on this important subject from selected members of staff.

Please note that the study will be conducted as an academic research and the information provided will be treated in strict confidence. Strict ethical principles will be observed to ensure confidentiality and the study outcomes and reports will not include reference to any individuals.

Your acceptance will be highly appreciated.

Yours Sincerely

Lawrence Mwagoti

APPENDIX III: Questionnaire

Section A: General Information

1. Name of the Company _____
2. How long has the company been in operation? _____
3. Gender [ ] Female [ ] Male
4. Age of the respondent (years) _____
5. Highest level of education attained [ ] Secondary [ ] College [ ] University

   [ ] Post Graduate [ ] Doctorate
6. Job title or position of the respondent in the organization. _____
7. How many employees are in the organization?_____
8. How would you classify your organization in regard to ownership?

   [ ] Locally owned [ ] Foreign-owned [ ] Combination of local and foreign [ ] other: Please specify _____
9. How would you describe the nature or the type of products/ services that you sell to your customers? _____
10. What type of eCommerce firm is your business? [ ] Click-only (conduct 'most' of your business online) [ ] Click and Mortar (sell online and have physical premises).
11. Which modes of payment do you accept from your customers? [ ] Cash [ ] Cheque

    [ ] Mobile payments [ ] Credit cards [ ] Debit cards [ ] Online payment systems [ ]

    Other [ ]
12. How do you deliver purchased goods to your customers? [ ] Door delivery [ ] Pick up [ ] Door delivery or Pick up [ ]

Section B: Models of eCommerce

13. Which model of eCommerce is your firm using?

    [ ] B2B eCommerce (refers to commercial transactions between businesses.)

    [ ] B2C eCommerce (retailing transactions between organizations and individual shoppers.)

[ ] C2C eCommerce (transactions between consumers, the eCommerce website serves to facilitate the transaction.)

Section C: Evaluating Social Engineering risks

14. What are the **different Social Engineering risk** do your organization encounter during its day-to-day activities? Tick where appropriate from the choices given below.

    1. Phishing/Spear phishing (Receiving e-mails that appear to be from reputable sources with the goal of influencing or gaining personal information) [ ]
    2. Baiting/ Trojan horse (Inquisitiveness of the victim to click and aid installation of malware on the targeted computer) [ ]
    3. Pretexting/Reverse social engineering (Obtaining information under false pretense) [ ]
    4. Social Media/ Fraudulent websites (An attack that uses social media sites such as Facebook and other fraudulent websites into misleading the casualty into clicking on a link that downloads malware to the victim's computer) [ ]
    5. SMSishing (Attack or fraudulent messages sent via SMS) [ ]
    6. Search Engine poisoning (Attack that happens when user clicks on the search engine result believing the query to be relevant to his search, but then he is redirected to another website that persuades him to download malware unknowingly.) [ ]
    7. Diversion Theft (Redirecting a courier or transport delivery to another location) [ ]

    Any other Social Engineering risks not mentioned above.

    _____

    _____

    _____

    _____

    _____

15. What losses do your organization suffer as a result of Social Engineering**?** Tick against the choices given below.

    1. Financial Loss [ ]
    2. Leaking of personal and business-sensitive data [ ]
    3. Negative reputation to the organization, for instance, decrease customer [ ]

loyalty

4. Network and system resources [ ]

5. Theft of goods [ ]

Any other Social Engineering loses not mentioned above

Section D: Determining Exposure

16. To what extent would you say to have used the following process to **determine exposure** of sensitive data to social engineering attackers? Indicate according to the scale shown below:
    1 -not at all

    2 -to a small extent

    3 -to a moderate extent

    4 -to a great extent

    5 -to a very great extent

Determining exposure	**1**	**2**	**3**	**4**	**5**
a) Periodically test and check privacy and information security controls (e.g. through the use of real-life simulation) to validate their effectiveness?					
b) How often do you conduct internet searches to locate and remove information that is in public domain or visible to the public?					
c) Do you conduct regular searches of the information system and physical storage to identify personally identifiable information that may be outside approved areas?					
d) How often do you check your website if it's listed in hacking forums?					
a. **Any other exposure determinant was not mentioned above**	**1**	**2**	**3**	**4**	**5**

Section E: Evaluating Defence

17. To what extent would you say to have used the following process to **evaluate defense** of sensitive data to social engineering attackers? Indicate according to the scale shown below:
    1 -not at all

    2 -to a small extent

    3 -to a moderate extent

    4 -to a great extent

    5 -to a very great extent

Evaluating defence	**1**	**2**	**3**	**4**	**5**
a) Document personal data and other sensitive information maintained by your organization, where is stored and how it's kept secure					
b) Conduct regular social engineering risk assessment and evaluate privacy threats for your organization, contractors & business partners					
c) Review who is approved to access sensitive information and personally identifiable data					
d) Review separation of duties to help ensure integrity of security checks and balances					
e) Implement mitigation controls designed to prevent and detect unauthorized access, theft or misuse of personally indefinable data & other sensitive data?					
f) Implement security controls, such as encryption of sensitive data in motion & at rest?					
g) Regularly review and keep up-to-date data destruction policies, to minimize risk of data breaches through unauthorized access to archived media or computers that are no longer in use.					
Any other evaluating defense process not mentioned above?					

Section F: Educate workforce.

18. To what extent would you say to have used the following process to **educate workforce** about social engineering? Indicate according to the scale shown below:
    1 -not at all

    2 -to a small extent

    3 -to a moderate extent

    4 -to a great extent

    5 -to a very great extent

Educating workforce	**1**	**2**	**3**	**4**	**5**
a) Provide mandatory social engineering and information security training on recurring basis to all employees and other staffs involved					
b) Do you communicate and post social engineering policies to customers and users (For instance , on the organization's website, or on a bulletin board at the office, through statements inserted in documents or emails)					
c) Clearly defining and making easily accessible process for reporting privacy incidents and complaints (Depending on the nature of the event, this may include reporting to the authorities, public and/or individuals)					
Any other educating workforce process not mentioned above?					

Section E: Streamlining technology and policy

19. To what extent would you say to have used the following process to **streamline technologies and policies** in your organization in regards to social engineering? Indicate according to the scale shown below:

1 -not at all

2 -to a small extent

3 -to a moderate extent

4 -to a great extent

5 -to a very great extent

Streamlining technology and policies	**1**	**2**	**3**	**4**	**5**
a) Employ automated tools, like Intrusion detection/prevention systems, next generation firewalls, to monitor and alert about suspicious or anomalous activity					
b) Use Data loss prevention solutions to track the movement and use of information within your system and prevent the unintentional disclosure of personal sensitive data, for both data at rest and data in motion					
c) Conduct policy violations to determine if they are well utilized?					
d) Periodically update and document new policies, regarding social Engineering threats noted and documented					
Any other streamlining technologies and policies not mentioned above?					