UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING AND INFORMATICS

SOCIAL ENGINEERING: MANAGING THE HUMAN ELEMENT OF INFORMATION SECURITY IN THE ORGANIZATION

By

MACHARIA KIAMA

P54/65237/2013

Supervisor

Dr. ELISHA ABADE

March, 2016

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

DECLARATION

I hereby declare that this project is my original work and has not been submitted for examination in this University or elsewhere for an award of any other degree.

Signed_____ Date_____

Macharia Kiama
P54/65237/2013

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

Signed_____ Date_____

Dr. Elisha Abade
School of Computing and Informatics

ABSTRACT

A definition given by European Network and Information Security Agency social engineering refers to techniques that exploit human weaknesses and manipulate people into breaking normal security procedures (ENISA, 2008, p. 7).

We can therefore say that organizations are still at risk because the people entrusted to safeguard their information are highly vulnerable to social engineering attacks. In this regard the study offered guidelines on how stakeholders can manage the social engineering threat within the organizations' risk appetite.

The general objective of the study focused on social engineering as a security threat in the organization and how human behavior contributes to its success. The specific objectives explored social engineering techniques, highlighted motives and factors that influence the success of social engineering attacks, determined risk areas that needed to be improved and modelled a risk matrix of probability of compromise/breach involving stakeholders and finally recommended guidelines on how the threat level of social engineering may be reduced in the organization.

This study adopted a hybrid of quantitative and qualitative methodologies and targeted the stakeholders of a general insurance company whose headquarters are situated in Nairobi. The study being descriptive was observational and also made use of questionnaires. The collected data was coded and entered into the Statistical Package for Social Sciences (SPSS) for analysis.

The output presented by these techniques indicate that social engineering being a 'non-technical' way of infiltration should be taken seriously as any other technical threat. It is therefore important for continuous research to be carried out in this field as the field of social engineering is dynamically changing with the advancement of technology. Further recommendations on how the social engineering threat level could be reduced were also provided by customizing elements of Enterprise Risk Management (ERM) Integrated Framework of the Committee of Sponsoring Organizations (COSO).

DEDICATION

To my family, friends and acquintances for the motivation
And
To the dynamic global information security industry.

ACKNOWLEDGEMENT

I am forever grateful to my friends, fellow students, colleagues at The University of Nairobi; School of Computing and Informatics, supervising and examining panel who were all key to the success of the research process.

- My supervisor Dr. Elisha Abade for the great insight given during the consultation sessions. You opened up many dynamics that can be explored in terms of Social Engineering.
- The panelists in general for the positive criticisms accorded during the presentations.

TABLE OF CONTENTS

LIST OF TABLES AND FIGURES

LIST OF ACRONYMS

ANOVA-Analysis of Variance

AV-Anti Virus

COBIT-Control Objectives for Information and related Technology

COSO-Committee of Sponsoring Organizations

CVI-Content Validity Index

DOS-Denial of Service

ENISA- European Network & Information Security Agency

ERM- Enterprise Risk Management

ID-Identity

IDS-Intrusion Detection System

IM-Identity Management

IPS-Intrusion Prevention System

ISO-International Standards Organization

ITIL-Information Technology Infrastructure Library

SE-Social Engineering

SPSS-Statistical Package for Social Sciences

SSO-Single Sign On

VM-Vulnerability Management

CHAPTER 1-INTRODUCTION

1.1 Background to the Study

A definition given by European Network and Information Security Agency social engineering refers to techniques that exploit human weaknesses and manipulate people into breaking normal security procedures (ENISA, 2008, p. 7). The scale and sophistication of related attacks is increasing, with even more avenues being exploited to reach users (including email, instant messaging, and social networking sites). Successful social engineering can be seen to rely upon a number of factors, including a convincing pretext for contacting the target, potentially accompanied by a degree of background research and/or the exploitation of current events. In addition, attackers are readily able to exploit psychological factors and human behaviour, as well as users‘(mis)understanding of the technology that they are required to use.

This may involve convincing them to perform non-typical actions or to divulge confidential information. Such attacks have become a long-standing problem in the security domain, and attackers essentially recognize that it is often easier to exploit the users of a system rather than the technology itself. However, despite its longevity, it is an area in which organizations often fail when it comes to protection.

Looking at where organizations invest their money on security, it is clear that the technology aspects receive far more attention than the people. Focusing primarily upon technical aspects of security and overlooking human vulnerabilities can easily leave them with controls that are still unable to prevent incidents. Indeed, why would someone need to defeat technologies such as firewalls, authentication, intrusion prevention and encryption in order to break into a system or steal information when they can just target the weakest link; the employees? Such realizations are certainly no secret amongst the attacker community (ENISA, 2008, p. 9) .

Security is all about knowing who and what to trust: Knowing when, and when not, to take a person at their word; when to trust that the person you are communicating with is indeed the person you think you are communicating with; when to trust that a website is legitimate or not; when to trust that the person on the phone is or isn’t legitimate; when providing your information is or isn’t a good idea. (Rohita, 2013)

Security is too often merely an illusion, an illusion sometimes made even worse when gullibility, naiveté, or ignorance come into play. In the end, social engineering attacks can succeed when people are stupid or, more commonly, simply ignorant about good security practices. With the same attitude as our security-conscious homeowner, many information technology (IT) professionals hold to the misconception that they've made their companies largely immune to attack because they've deployed standard security products - firewalls, intrusion detection systems,

or stronger authentication devices such as time-based tokens or biometric smart cards. Anyone who thinks that security products alone offer true security is settling for the illusion of security. It's a case of living in a world of fantasy: They will inevitably, later if not sooner, suffer a security incident. (Mitnick & Simon, 2002)

As noted security consultant Bruce Schneier (cited in (Mitnick & Simon, 2002)) puts it, "Security is not a product, it's a process." Moreover, security is not a technology problem - it's a people and management problem.

As developers invent continually better security technologies, making it increasingly difficult to exploit technical vulnerabilities, attackers will turn more and more to exploiting the human element. Cracking the human firewall is often easy, requires no investment beyond the cost of a phone call, and involves minimal risk

In Kenya the continued adoption rising of online/mobile banking and continued popularity of Mobile Money in the region is opening new frontiers in social engineering from which malicious attackers can obtain financial information or money itself from unsuspecting users. According to the Kenya Cyber Security Report (Kigen, et al., 2014), the continued adoption of online and mobile banking services is leading to new threats for customers and local financial institutions'. Many financial institutions are introducing vulnerable web and mobile applications. In a recent study 33 online banking portals were sampled. Out of the 33 banking applications sampled, only 2 banking portals had adequate online security deployed on their web application. Majority of the web applications reviewed lack of strong encryption and are susceptible to phishing attacks. The continued popularity of Mobile money adoption in the region has also attracted criminals who are now targeting this new money transfer channel. In 2013, an increase in mobile money fraud was noted targeting individuals and organisations. The fraudsters are getting innovative and are very fast on finding loopholes in new controls implemented by merchants, banks and consumers. A typical scenario in mobile money fraud is where the conmen will use SMS and USSD codes, and pose as customer care officials from leading service providers. They lie to clients that they have won money and even go as far as warning them against sharing their PIN as an assurance.

The unsuspecting customers are then duped into entering their PIN codes 'to check' if they had received the money.

This is after they are asked to dial 5555555 to have the money transferred to their accounts.

Apparently, the conmen and women send a secret password to a customer's phone with a code named 'Equity Bank' which they tell them to use.

It is suspected that customers will enter the password that gives the fraudsters access to their accounts and can withdraw money remotely through ATMs.

The fraudsters will thereafter withdraw money as long as they have the code and the mobile number. (Anon., 2014) This is a social engineering scheme and is not associated with any system weakness or hacking but weakness of the human element.

1.2 Statement of the Problem

Despite companies investing immensely in the technical aspect of security, organizations are still at risk of attacks from hackers. Securing the hardware, software and firmware is relatively easy; it is the human factor that causes security experts the biggest challenge. The human element is usually the weakest link in the security chain. In the 1970s, we were told that if we installed access control packages then we would have security. In the 1980s we were encouraged to install effective anti-virus software to ensure that our systems and networks were secure. In the 1990s we were told that firewalls would lead us to security. Now in the twenty-first century, it is intrusion detection systems or public key infrastructure that will lead us to information security. In each iteration, security has eluded us because the silicon based products have to interface with carbon-based units. (Peltier, 2014)

It is the human factor that will continue to appear in the discussion on social engineering. A skilled social engineer will often try to exploit this weakness before spending time and effort on other methods to crack passwords or gain access to systems. Why go to all the trouble of installing a sniffer on a network, when a simple phone call to an employee may gain the needed User ID and password?

We can therefore say that organizations are still at risk because the people entrusted to safeguard their information are highly vulnerable to social engineering attacks. In this regard the study is offering guidelines on how stakeholders can manage the social engineering threat within the organizations' risk appetite.

1.3 Objectives of the Study

The general objective of the study focused on social engineering as a security threat in the organization and how human behaviour contributes to its success.

Specific objectives:

i. Explore the various ways that a social engineer may use to infiltrate the organization's security perimeter.
ii. Highlight the motives and factors that influence the success of a social engineering attack.
iii. Determine the risk areas that need to be improved and model a risk matrix of the probability of compromise/breach involving stakeholders.
iv. Recommend guidelines on how the threat level of social engineering may be reduced in the organization.

1.4 Research Questions

i. What are the various ways that a social engineer may use to infiltrate the organization's security perimeter?
ii. What are the motives and factors that make social engineering attacks successful?
iii. What are the risk areas in the organization and what is the probability of compromise/breach involving stakeholders?
iv. How can the threat level in the organization be reduced?

1.5 Justification for the Study

The proposed study intends to contribute towards a better understanding of the risks associated with successful social engineering attacks in the organization. The benefits will not be confined to organizations but will extend to individuals as well.

By understanding the various ways that a social engineer may use to gain information and also the factors that make social engineering attacks so successful, they can tailor their policies on how to best manage the threat in a proactive and not a reactive manner.

The study is not only useful in an insurance company setting but can be applicable in any industry after appropriate customization.

1.6 Scope

The study was carried out in an insurance company in Kenya. The company is licensed to transact in general insurance business and has its headquarters in Nairobi with a network 26 branches countrywide. With a staff workforce that has over 300 permanent members it was an ideal place to carry out this particular study.

CHAPTER 2-LITERATURE REVIEW

2.1 Introduction

Information Security is simply the process of protecting information availability, data integrity, and privacy.

No collection of products or technologies alone can solve every information security problem faced by an organization. Effective information security requires the successful integration of security products such as firewalls, intrusion detection systems, vulnerability scanners and technologies such as authentication, encryption and also security policies and procedures

Information security can also be described as a complex system, made up of hardware, software, and wetware. Hardware primarily includes the computer systems that we use to support our environments. Software includes all of the code, databases, and applications that we use to secure the data. Wetware includes policy, procedure, training, and other aspects that rely on people.

The threat environment we're seeing today is radically different from what existed even just six months ago. Six months from now, one is expected to say the same thing. The actors behind the threats are also evolving; the motivation behind attacks is more difficult to predict and anticipate. Beginning in 2005, methods for executing internet attacks have been quietly evolving. The shift has remained subtle to date but enterprises that ignore newer attack methods may experience significant losses. Hackers' motivation for launching attacks has changed, causing the current threat evolution. Today attacks are profit driven, not glory and fame. The more organized attempts for financial gain are harnessing intellectual talent within the hacker community to devise new attack strategies and innovative malicious code (malcode) that invades enterprises' systems without detection. (IBM Global Technology Services, 2007, p. 1)

Information security solutions used to protect organizations from hackers intending to generate front page news about a successful denial of service attack or a website defacement. In the new era of internet threats, attackers are motivated by profit or politics and use cutting edge technology to probe networks undetected for as long as possible. The longer attacks go unnoticed, the more opportunity for success in data theft and other proof generating activities. (IBM Global Technology Services, 2007, p. 1)

Table 1 illustrates how today attacks differs from earlier attacks.

Attack Characteristics	Earlier Attacks	New Era Attacks
Motivation	Glory and fame	Profits
Complexity	One dimensional i.e exploits only one vulenrability	Multi faceted attack exploits multiple vulnerabilities
Scope	Widespread for maximum publicity (carpet bombing or shotgun approach)	Targeted attacks to go unnoticed (surgical strikes or sniper approach)
Primary Risk	Network downtime to clean and repair	Direct financial loss; Theft of trade secrets or corporate strategy; Customer data breaches and disclosure
Targets of Attack	High profile / Widespread	Laser focus on firms or individuals
Effective Defense	Anti-Virus Signatures; Reactive Approach	Multi layer protection; Pre-emptive and behavioral approach required
Recovery	Scan and Remove	Not always possible; may require re-image of system
Types of Attacks	Virus, Worms, Spyware	Designer Malware, Root kits, Ransomware, Spear Phishing
Attack Approach	Network Traffic – Tell everyone the threat is here	Malicious Code – Stealth like operation to avoid discovery

Table 1: Evolution of Attacks

(IBM Global Technology Services, 2007, p. 1)

2.2 Common Information Security Terms

Confidentiality refers to information protection from unauthorized read operations.

Privacy is often used when data to be protected refers to individuals.

Integrity refers to information protection from modifications and it involves several goals which are assuring the integrity of information with respect to the original information (relevant especially in web environment) – often referred to as *authenticity*, protecting information from unauthorized modifications and protecting information from incorrect modifications – referred to as *semantic integrity.*

Availability ensures that access to information is not denied to an authorized subject.

Information Quality is not considered traditionally as part of information security but it is still very relevant.

Completeness ensures that subjects receive all information they are entitled to access, according to the stated security policies.

User authentication is the act of verifying the identity of subjects wishing to access the information.

Information authentication ensures information genuineness which is supported by signature mechanisms.

Encryption refers to protection of information when being transmitted across systems and when being stored on secondary storage.

Intrusion detection protects against impersonation of legitimate users and also against insider threats (Kantarcioglu, n.d.).

2.3 Classes of Threats

i. *Disclosure*

Deception contains elements such as snooping and Trojan horses.

Snooping which is the unauthorized interception of information, is a form of disclosure. It is passive, suggesting simply that some entity is listening to (or reading) communications or browsing through files or system information. *Wiretapping*, or *passive wiretapping*, is a form of snooping in which a network is monitored. (It is called "wiretapping" because of the "wires" that compose the network, although the term is used even if no physical wiring is involved.) Confidentiality services counter this threat. (Bishop, 2004)

Trojan Horses are programs in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. (Rouse , 2015)

ii. *Deception* contains elements such as modification, spoofing, repudiation of origin and denial of receipt.

Modification- Unlike snooping, modification is active; it results from an entity changing information. *Active wiretapping* is a form of modification in which data moving across a network is altered; the term "active" distinguishes it from snooping ("passive" wiretapping). An example is the *man-in-the-middle* attack, in which an intruder reads messages from the sender and sends (possibly modified) versions to the recipient, in hopes that the recipient and sender will not realize the presence of the intermediary. Integrity services counter this threat. (Bishop, 2004)

Spoofing- an impersonation of one entity by another, is a form of both deception and usurpation. It lures a victim into believing that the entity with which it is communicating is a different entity. Integrity services (called "authentication services" in this context) counter this threat. (Bishop, 2004)

Repudiation of origin refers to a false denial that an entity sent (or created) something. Integrity mechanisms cope with this threat. (Bishop, 2004)

Denial of receipt refers to a false denial that an entity received some information or message. Integrity and availability mechanisms guard against these attacks. (Bishop, 2004)

iii. Disruption

Modification is a major element.

iv. Usurpation- wrongful or illegal encroachment, infringement, or seizure.

It can contain elements of modification, spoofing and delay.

Delay refers to a temporary inhibition of a service. Typically, delivery of a message or service requires some time *t*; if an attacker can force the delivery to take more than time *t*, the attacker has successfully delayed delivery. Availability mechanisms can thwart this threat. (Bishop, 2004)

Denial of service is a long-term inhibition of service. The attacker prevents a server from providing a service. The denial may occur at the source (by preventing the server from obtaining the resources needed to perform its function), at the destination (by blocking the communications from the server), or along the intermediate path (by discarding messages from either the client or the server, or both). Denial of service poses the same threat as an infinite delay. Availability mechanisms counter this threat (Bishop, 2004).

2.4 Goals of Security

Prevention: Prevent attackers from violating security policy

Detection: Detect attackers' violation of security policy

Recovery: Stop attack, assess and repair damage. Continue to function correctly even if attack succeeds.

Information must be protected at various levels:

HOST refers to the systems responsible for the housing of digital assets. HOSTS petition access to NETWORKS and DATA as instructed (either directly or indirectly) by a human. They are the endpoint for access to digital assets from other petitioners. A personal computer running Windows and Internet Explorer, being operated by a human, is an example of a HOST. A "Smart Phone" accessing mail via Outlook Mobile Access is a HOST. A high-end, multiprocessor server in a datacentre is a HOST. A laptop in a lead suitcase is a HOST. A Storage Area Network (SAN) is also a HOST (Hitchcock, 2005).

NETWORK refers to all systems, devices, technologies, and equipment responsible for transporting data between HOSTS. A router is NETWORK. Cat-5 and fibre-optic cabling are NETWORK, as are Wi-Fi RF spectrum, phone lines and phone switches, and GPS signalling. A network-based firewall appliance is NETWORK. (Hitchcock, 2005)

DATA refers to the actual bits-and-bytes that represent human-created and/or human relevant information. All digital assets consist wholly of DATA. A Word document on a hard drive or in a computer's memory is DATA. An analog phone conversation being transmitted over copper is

DATA. The result of a SQL Server query as displayed on a computer workstation is DATA (Hitchcock, 2005).

PHYSICAL PROTECTION of the perimeter is also important

2.5 Enforcing Information Security Mechanisms

Confidentiality is enforced by the access control mechanism

Integrity is enforced by the access control mechanism and by the semantic integrity constraints

Availability is enforced by the recovery mechanism and by detection techniques for DoS attacks – an example of which is query flood

According to the Bitpipe Research Guide on Security Overview (Bitpipe, n.d.), protecting corporate information and technology assets from intruders, thieves, and vandals is a significant challenge for most enterprises. Historically, investments in security technology were made by individual technology managers and business units in response to the specific threats they faced. CIOs are now implementing technologies that can support the centralized management and enforcement of security policy. As a result, the fragmented security market is coalescing around four primary solution sets: Identity management to authorize user access to system resources, Vulnerability Management to uncover and remedy threats early, Threat Management to respond to intrusions and attacks on the network and Trust Management to securely exchange information over public networks.

Identity Management (IM) solutions are responsible for authenticating and authorizing the network-based users who need to use online services and resources (Bitpipe, n.d.). Identity Management solutions generally include:

Provisioning which is the process of granting and revoking the appropriate access rights and privileges to employees, customers, suppliers, and business partners.

Web access control products provide centralized and automated management to validate a user, and then permit the user to access resources in the environment for which that user has been granted permission**.**

Single Sign-On (SSO) allows a user to log onto every assigned system that user has access to once, using a single user ID and password combination.

Vulnerability Management (VM) helps the enterprise identify vulnerabilities or weaknesses in the computing environment, and provide the infrastructure to eliminate them (Bitpipe, n.d.). Vulnerability Management solutions generally include:

Firewalls refer to a system or group of systems that enforces an access control policy between two networks. The firewall has a dual role as the mechanism that exists both to block and to permit traffic attempting to access network resources.

Vulnerability assessment tools evaluate and monitor operating systems and applications for needed fixes to known problems, such as viruses, worms, unsecured backdoors, and security holes.

Network vulnerability scanning is the process of checking for all the potential methods an attacker might use to tamper with an organization's network by analyzing the types of software and system configurations on a given network.

Threat Management focuses on identifying and responding to anomalous and malicious events that occur throughout the network (Bitpipe, n.d.). Threat Management solutions generally include a combination of intrusion detection and security event management technology.

Intrusion Detection systems monitor network traffic, verify the integrity of system files, monitor network event logs, and may also include deception systems to lure and trap hackers.

Security Event Management products actively monitor IT resources across an organization, filter and correlate events, and automate responses to security incidents.

Trust Management is the practice of protecting and enabling activities that are of high risk to the enterprise (Bitpipe, n.d.). These solutions rely on encryption and access control techniques to create a secure process for authorized individuals. Trust Management solutions generally include:

Public-Key Infrastructure (PKI) is the combination of encryption technologies, digital certificates, and certificate authorities that allows enterprises to protect the security of their communications and business transactions on the Internet.

Virtual Private Network (VPN) is a private data network that uses the public telecommunication infrastructure (as opposed to a system of owned or leased lines), maintaining privacy through the use of a tunneling protocols and security procedures.

2.6 Information Security in the Insurance Sector

According to The Deloitte Global Cyber Executive Briefing on Insurance (Deloitte, 2015), cyber-attacks in the insurance sector are growing exponentially as insurance companies migrate toward digital channels in an effort to create tighter customer relationships, offer new products and expand their share of customers' financial portfolios. This shift is driving increased investment in traditional core IT systems (e.g., policy and claims systems) as well as in highly integrated enabling platforms such as agency portals, online policy applications and web- and mobile-based apps for filing claims. Although these digital investments provide new strategic capabilities, they also introduce new cyber-risks and attack vectors to organizations that are relatively inexperienced

at dealing with the challenges of a multi-channel environment. What's more, the challenges are likely to become more complex as insurers embrace big data and advanced analytics that require collecting and handling vast amounts of consumer information. As insurers find new and innovative ways to analyze data, they must also find ways to secure the data from cyber-attacks.

Cyber-criminals have started to recognize that insurers possess large amounts of personal information about their customers, which is very attractive to identity thieves and fraudsters. In some cases, insurers also possess significant amounts of customer credit card and payment data. However, there is at least one case in the insurance sector where the victims of a cyber-attack weren't even paying customers but merely consumers who had requested a price quote.

Cyber-criminals targeting insurers often have significant resources. This enables them to employ sophisticated attacks that combine advanced malware with other techniques such as social engineering.

Attacks on insurance firms can result in significant, tangible damages such as fines, legal fees, lawsuits and fraud monitoring costs. However, a less obvious but no less significant impact may be loss of trust, driven by customers' concerns about whether their information is truly safe. Since the insurance business revolves around trust, a major breach can have a very real impact on an insurer's brand and market value.

It's worth noting that most of the breaches publicly reported by insurance companies to date have been characterized as short term attacks, with cyber-criminals compromising a system, stealing specific information and then quickly moving on. In fact, the research did not uncover any documented cases of long-term infiltration and cyber-crime in the insurance sector. However, it is believed the number of long-term attacks may be silently growing as attackers quietly slip in undetected and establish a persistent, ongoing presence in critical IT environments.

Over the years, many insurance organizations have invested a lot of money in security tools and processes that may be providing a false sense of security. As attackers learn to leverage encryption and other advanced attack techniques, traditional tools such as firewalls, antivirus software, intrusion detection systems (IDS) and intrusion prevention systems (IPS) are becoming less and less effective. As a result, many insurers may be misallocating their limited resources to address compliance-oriented, easily recognized threats while completely overlooking stealthy long-term threats that ultimately could be far more damaging.

No matter how secure a system is, there's always a way to break through. Often, the human elements of the system are the easiest to manipulate and deceive. Creating a state of panic, using influence, manipulation tactics, or causing feelings of trust are all methods used to put a victim at ease. The first step in becoming more secure is simply conceding that a system is vulnerable and

can be compromised. On the contrary, by believing a breach is impossible, a blindfold is placed over your eyes as you run full speed ahead.

A social engineering hacker attempts to persuade your staff to provide information that will enable him or her to use your systems or system resources. Traditionally, this approach is known as a *confidence trick*. Many midsize and small companies believe that hacker attacks are a problem for large corporations or organizations that offer large financial rewards. Although this may have been the case in the past, the increase in cyber-crime means that hackers now target all sectors of the community, from corporations to individuals. Criminals may steal directly from a company, diverting funds or resources, but they may also use the company as a staging point through which they can perpetrate crimes against others. This approach makes it more difficult for authorities to trace these criminals.

To protect your stakeholders from social engineering attacks, they need to know what kinds of attack to expect understand what the hacker wants, and maybe estimate what the loss might be worth to your organization. With this knowledge, policy makers and security professionals can augment the security policy to include social engineering defenses.

A social engineer runs what is typically known as a "con game". A person using social engineering to break into a computer network generally gains the confidence of someone who is authorized access to the network, in order to help reveal information that compromises that networks security. With the Internet's current proliferation of poorly-secured computers and "many" well known security holes, the majority of security compromises are now done by exploiting vulnerable computers. However, social engineering remains extremely common and is a common way to attack systems protected by other methods.

An attacker may seem respectable, possibly claiming to be a new employee, a repair person or a consultant and even providing phony credentials to support that identity. By asking the right questions, the attacker may be able to piece together enough information to aid in their infiltration of an organizations network. If an attacker is not able to gather enough information from one source, they will contact another source within the same organization and rely on the information from the first source to add to their appearance of credibility.

In today’s ever changing world security should be everyone’s responsibility and not a preserve of security professionals. It is important for everyone to be to be familiar with Social Engineering techniques and the counter-measures available to reduce the likelihood of success. A workplace may have otherwise excellent security, but if a help desk worker readily gives out or resets lost passwords, or employees let others tailgate on their opening secure doors with their key-card, security can be horribly compromised. Despite the robustness of a firewall, if a single user has

hardware (e.g. a modem) or software (e.g. some file sharing software) that allows bypassing the firewall, a hacker may gain access with catastrophic results (Hadnagy, 2011, pp. 17-20).

2.7 Social Engineering Techniques

These are merely the different psychological tricks an attacker can deploy to persuade a user to give out information needed to gain access to a computer or network. By nature, humans are helpful and when asked to give out information, we tend to give out this information willingly. The attacker preys on the user's sympathy to be helpful. Sometimes, it could be out of fear of getting into trouble if reported to senior person that a user is not cooperating.

Social engineers deploy various skills as a form of persuasion. The following are some of these techniques.

Hoaxing is a trick that's makes people to believe that something false is genuine. Social engineers create fake situations in order to lead a user into a change of decision on a certain matter due to a fear of an untoward incident (Mugala, 2014).

Dumpster Diving is the searching of physical or electronic junk or trash to look for information. A dumpster can be searched for paper documents that are readable and contain valuable information. Electronically, the recycle bin on a user's can be searched for sensitive and private data. From this information, an attacker can carry out identity theft (Mugala, 2014).

Shoulder Surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand (Rouse, 2014).

Phishing and Emails. Phishing is an e-mail fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients. Typically, the messages appear to come from well-known and trustworthy Web sites. A phishing expedition, like the fishing expedition it's named for, is a speculative venture: the phisher puts the lure hoping to fool at least a few of the prey that encounter the bait (Rouse, 2014).

Pharming is a scamming practice in which malicious code is installed on a personal computer or server, misdirecting users to fraudulent Web sites without their knowledge or consent. Pharming has been called "phishing without a lure." (Rouse , 2015).

Vishing is the telephone equivalent of phishing. Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit (Webopedia, 2015).

Impersonation of staff and identity theft. This can be done via telephone, email or even face to face. An attacker can pretend to be someone else in a very convincing way. A social engineer can go as far as creating a fake user Identity card, email address or pretending to be another person on the phone. If the impersonation is successful, intimidation tactics and blackmail can be deployed and with this a user will have no option but to give the required information. A common technique for impersonation is clouting. This is having authority over an individual by posing as an authoritative figure such as a manager or anyone senior. With this stance, a social engineer is capable of gaining a lot of information (Mugala, 2014).

Windows popups. An attacker's malicious software can generate a pop up window which can prompt a user to reenter his or her username and password. Once this information is entered, the attacker gets hold of it and from here is able to do anything. The user will not realize that an attack was carried out and continue with their work (Mugala, 2014).

2.8 Motives of a Social Engineering attack

Knowing why social engineers might attack is crucial for estimating the likelihood of a social engineering attack on a specific organization and to implement appopriate measures and controls to counter this attack.

The motives of the social engineer can be classified in various categories. For each category a general description of the motive is given, a classification in malicious or good intentions and what social engineering can play in an attack with this motive (Oosterloo, 2008).

Financial Gain. These attackers are after financial gain and focus on money, valuable data, services, capacity or intellectual property, extortion, fraud and marketing schemes. This kind of attack requires a great deal of planning and preparation to be a success and to remove all traces that could lead back to the attacker. The intentions of the attacker are malicious, the target will always be harmed and suffer financial damage.Social engineering is a technique used extensively to gather information to prepare and execute the attack (Oosterloo, 2008).

Personal Interest. This includes entertainment and curiosity. Attackers focus on the access, change or removal of information. Removing traces is not a high priority and it requires little preparation.

The intentions of the attacker are not malicious but an attack can still cause great damage. Social engineering can be used to gather information, prepare for another form of attack or be used to get final access, change or removal of information (Oosterloo, 2008).

External Pressure. This includes the pressure to demonstrate skills to stay or be accepted in a social group or upholding a certain status and with that power within the group. It also includes the pressure of relatives, friends and organized crime to influence an individual or organization. This can take on many forms for example blackmail. The motive is therefore the relief of part of the pressure by acquiring certain status within the social group. An individual can be pressured for example because of his/her place in the target organization; to misuse their social status or job function.

The intentions of the attacker are derived from the intentions of the social group or person that applies pressure. With organized crime it is clear that the intentions are malicious and will in the end harm an individual or organization. Social engineering can be used to gather information, prepare for another form of attack or be used to achieve the final goal of the attack (Oosterloo, 2008).

Intellectual Challenge. Attackers focused on an intellectual challenge are not necessarily after recognition. The attacker wants to prove something is possible and targets secure or high profile organizations and people. The intentions of the attacker are not by definition malicious but the technical tools used i.e. worms, viruses or Trojan horses can cause great damage or create vulnerabilities that can be abused by other attackers. The way social engineering can be used in an attack is subject to the goal of the attack; if the goal is to acquire specific information, social engineering can play a great part in the attack. But the main challenges taken up by attackers are still technical; in most cases therefore social engineering will be used to gather information and prepare for the final attack (Oosterloo, 2008).

Damage Containment. An attack can also focus on the minimization of damage from a previous attack that may have been malicious or try and help individuals and organizations to patch vulnerabilities in their systems and network. Although the intentions of these attacks are not malicious the outcome can still cause damage when the attack is performed with unfamiliar tools. By means of social engineering the attacker can for example help individuals and organizations to change their settings or delete malicious software. And it can again be used to gather information and prepare another form of attack (Oosterloo, 2008).

Personal Grievance. In this case grievances are very general and include claim of right, revenge and vigilantes. The attack is based on a feeling of injustice. Attacks can target an individual or organization to retrieve something that the attacker believes is his/hers, or just to damage the individual or organization that has caused this injustice. The intentions of the attacker are malicious because something is taken from the target or the attack causes harm, even though the attacker is alone in his/her perception of having suffered. Social engineering can be used to gather information, prepare another form of attack or be used to achieve the final goal of the attack (Oosterloo, 2008).

Politics. The causes that lay underneath these political attacks can be for example religious, political, environmental and can lead to extreme forms such as terrorism. The focus of the attack is in most cases an individual or organization that represents interests against their cause or is highly visible. Attacks on these people or organizations can generate great publicity to the cause. Cyber terrorists can cause massive damage for their beliefs and focus on critical infrastructure. The intentions are malicious as activists will do anything to get publicity for their cause. Social engineering can be used to gather information, prepare another form of attack or be used to achieve the final goal of the attack (Oosterloo, 2008).

2.9 Factors that influence the success of a social engineering attack

These are the elements that a social engineer may look for or exploit in a target when attempting an attack. They may be categorized as Personality Traits, Human Factors and Organizational Factors.

2.9.1 Personality Traits

Some researchers believe that personality traits may play a role in susceptibility to social engineering exploits (Alseadoon, et al., 2012).

Differences in personality may influence the manner in which people interact with others, approach decisions, and respond to job uncertainties or job pressures, and react to social engineering exploits. Contemporary personality theory classifies humans on five broad personality dimensions or traits (also called the Big Five personality factors). The common Big Five factor model (Digman, 1990) includes neuroticism, extraversion, openness to experience, agreeableness, and conscientiousness (also used, for example, in the work of McCrae and John (Macrae & John, 1992) and Weiner and Greene (Weiner & Green, 2008), which are defined below.

Neuroticism is the tendency to experience unpleasant emotions easily, such as anger, anxiety, depression, or vulnerability. It is sometimes called emotional instability, and people who score high on neuroticism are emotionally reactive and vulnerable to stress (lacking the ability to cope

effectively with stress, they may have a diminished ability to think clearly and make decisions). In contrast, people who score low on neuroticism tend to be more calm, emotionally stable, and free from persistent negative feelings. A study of phishing susceptibility and the Big Five personality traits found that neuroticism was most highly correlated to responding to a phishing email scheme (Halevi, et al., 2013).

Extraversion is the tendency to seek out the company of others; extroverts enjoy interacting with people and are perceived as being enthusiastic, action oriented, and full of energy. Extraverted personalities often seek excitement and tend to be assertive. Introverts have lower social engagement and energy levels than extraverts: They tend to seem quiet, low-key, deliberate, and less involved in the social world. Introverts are not necessarily shy or antisocial; rather they are more independent of their social world than extraverts. Parrish (Parrish, et al., 2009) suggests that extraversion can lead to increased phishing vulnerability, and they cite empirical research that found that high extraversion was associated with people giving up sensitive information (to gain acceptance to a social group).

Openness is associated with intellectual curiosity, creativity, an appreciation for different ideas and beliefs, a willingness to try new things, and the desire to seek out new experiences without anxiety. People with low scores on openness tend to have more conventional, traditional interests, and they tend to be conservative and resistant to change. Parrish speculated that because openness is associated with technological experience and computer proficiency, people who score high on openness could be less susceptible to social engineering attacks; on the other hand, they suggested that a general openness to all experiences and tendency toward fantasy could play into the criminal's hands (Parrish, et al., 2009). Two empirical studies tend to favor the hypothesis that openness contributes to social engineering susceptibility. A study with 200 Saudi Arabian students found a significant relationship between individuals scoring high on the openness personality trait and responding to a phishing email attack (Alseadoon, et al., 2012). Another study found that people who scored high on the openness personality factor post more information on Facebook and use less strict privacy settings (Halevi, et al., 2013).

Agreeableness is a tendency to be compassionate and cooperative rather than suspicious and antagonistic toward others. The trait reflects individual differences in general concern for social harmony. Agreeable individuals value getting along with others and are generally considerate, friendly, generous, helpful, and willing to compromise their interests with others. Agreeable people also have an optimistic view of human nature. Agreeableness is positively correlated with good teamwork skills, but it is negatively correlated with leadership skills. In contrast, a person who scores low on agreeableness may place self-interest above getting along with others. Less agreeable people tend to be distant, unfriendly, and uncooperative, and their skepticism about

others' motives might cause them to be suspicious. This trait may be the one most highly associated with social engineering susceptibility: Facets of agreeableness that would seem to be most vulnerable to phishing exploits are trust, altruism (belief in or practice of disinterested and selfless concern for the well-being of others), and compliance (Parrish, et al., 2009).

Conscientiousness focuses on self-discipline, dutiful action, and a respect for standards and procedures. This trait shows a preference for planned rather than spontaneous behavior.

People who score high on conscientiousness tend to be known for their prudence and common sense. People who score low on conscientiousness are typically more impulsive and spontaneous. People who are high in conscientiousness tend to take longer to make a decision; those low in conscientiousness are more likely to make a snap decision.

Presumably, higher levels of conscientiousness would make individuals more likely to follow training guidelines and less likely to break security policies (Parrish, et al., 2009). Consistent with this view, a study demonstrated that low levels of conscientiousness predicted deviant workplace behavior such as breaking rules or behaving irresponsibly (Salgado, 2002).

2.9.2 Human Factors

Lack of Attention. Dhamija and colleagues studied features of phishing websites to determine what users attended to in assessing the websites' legitimacy (Dhamija, et al., 2006). Participants were shown 20 websites and asked to identify which ones were fraudulent and which were authentic. They found that 23% of the 22 participants ignored browser-based security cues (address bar, status bar, Secure Sockets Layer [SSL] padlock icon); these individuals made incorrect choices 40% of the time. In addition to the problem of lack of attention to security cues, Dhamija also found that visual deception practiced by phishers could fool even the most sophisticated users.

A study by Vishwanath suggests that individuals focus disproportionately on urgency cues, often ignoring other elements of the email such as its source, grammar, and spelling (Vishwanath, et al., 2011). Because these other elements aid the detection of deceptive stimuli (Jakobsson, 2007), an individual's lack of attention to these elements may increase the individual's susceptibility to phishing. In addition, Vishwanath found that individuals were far more likely to respond to phishing emails when they were faced with large email loads.

Lack of Knowledge and Memory Failure. Consistent with research that contends users do not notice cues that should reveal suspicious or fraudulent phishing sites, Sharek reported that users lack knowledge about design inconsistencies that distinguish real and fake error messages (Sharek, et al., 2008). Based on research relating attentional processes to phishing susceptibility, key knowledge elements include knowledge about security features and understanding of URL and domain name syntax (Dhamija, et al., 2006). Research supports the claim that experience *does*

have a positive effect: previous exposure to phishing attacks makes users less likely to respond to phishing exploits in the future (Downs, et al., 2007).

Faulty Reasoning or Judgment. Errors in judgment and reasoning can occur when the individual experiences cognitive bias.

Several types of cognitive bias exist, but the prominent types include attentional bias, memory bias, and decision-making biases. Kahneman and Tversky have shown that people's decisions are often biased and are not purely rational (i.e., all decision options being systematically considered and decisions being made based on factual reasoning) (Kahneman & Tversky, 1979). An example of decision-making bias occurs when individuals tend to think that threats are highly unlikely (e.g., they underestimate the abilities of social engineering attackers and overestimate the defensive capabilities of organizational security systems) and consequently ignore such threats (Sandouka, et al., 2009). Also, some users feel that use of strong security features will impede their job (Erkkila, 2011). Annoyance with popup messages may actually lead (impatient) users to click on fake popups (Sharek, et al., 2008), which contributes to poor judgment in assessing risks.

Risk Tolerance and Poor Risk Perception. The National Institute of Standards and Technology (NIST) defines risk as the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence (NIST, 2002). From a cognitive process point of view, risk-taking behavior is a function of risk perception (a decision maker's assessment of the risk inherent in a situation), risk propensity (the general tendency either to take or to avoid risk), and a decision process (determining how to act in the face of a risky situation). Considering risk propensity, high-risk or risk-tolerant individuals may take big risks despite cybersecurity training, while risk-averse individuals are less likely to knowingly take risky actions. People who are less risk averse are more likely to fall for phishing schemes; those who are more risk averse are the less likely to do so (Sheng, et al., 2010).

Casual Values and Attitudes about Compliance. Employees whose attitudes and beliefs do not align with company security practices and policies and so fail to comply with them are a major threat to information-system security (Pahnila, et al., 2007). Employee attitudes (e.g., manner, disposition, feeling, and position, with respect to a person or thing) and normative beliefs (i.e., the perception of what other people believe) can impact the intention to comply with information system security policy (Bulgurcu, et al., 2010).

*Stress and Anxiety***.** Workplace stressors (e.g., organization-imposed time pressures) contributing to higher levels of subjective mental workload tend to negatively impact human performance by, for example, narrowing visual attention such that important cues attributed to malicious activity may be missed and by reducing cognitive resources needed for effective job. An obvious

implication is that reducing work-related stress levels by adjusting time pressure and workload is one way to reduce the likelihood of potential social engineering incidents.

2.9.3 Organizational Factors

Inadequate Management and Management Systems. Effective management includes practices to ensure the availability of qualified staff, assignment of tasks to staff who have appropriate capabilities and experience, and availability of materials and resources to complete the task.

The following are examples of management and management systems that not only reduce productivity and job satisfaction but also create conditions that promote human error:

Poor communication related to the task, confusing procedures or directions, tools or systems with design deficiencies (such as poor user interfaces and inadequate system feedback or status), problems with the work environment (e.g., noisy, hot, cold) and inadequate materials or resources (insufficient resources to successfully and efficiently complete the job). Most of these conditions have multiple deleterious effects on employee job performance and morale; a particularly harmful effect is increasing job stress (Leka, et al., 2004).

Insufficient Security Systems, Policies, and Practices. Another consideration relevant to organizational factors is the effectiveness of security practices, policies, and tools. Security practices are often difficult and confusing for an average computer user, and usage errors caused by these difficult security systems can yield serious consequences. In addition, an organization may provide inadequate or ineffective security through its policies (e.g., whether users are required to change passwords periodically) or its technical and defensive measures (such as firewalls or other computer security systems). At the other extreme, security systems, policies, or practices may be too strict or too difficult for most workers to follow, which also may undermine organizational security. Systems that are difficult to understand or use are negatively perceived by users and are less likely to be used. Difficulty using security systems may also encourage users to employ shortcuts around these system processes, which may make them more susceptible to social engineering incidents.

Job Pressure. Numerous workplace and environmental conditions have been implicated as sources of employee stress and fatigue. Although the definition of stress varies across research domains, there is broad agreement about conditions that cause stress. Studies consistently reported that time pressure and workload are major sources of stress. Time pressure negatively affects performance of even well trained individuals (Lehner, et al., 1997) which may make them more susceptible to social engineering incidents (Social Engineering Institute, 2014).

2.10 Why is Social Engineering a big deal in Security?

A combination of the above factors ensures that the threat of social engineering still remains to be a big headache to security experts globally. According to The Human Factor Report 2016 in 2015, social engineering was the number one attack technique. People replaced exploits as attackers' favorite way to beat cybersecurity. Attackers shifted away from automated exploits and instead engaged people to do the dirty work—infecting systems, stealing credentials, and transferring funds. Across all vectors and in attacks of all sizes, threat actors used social engineering to trick people into doing things that once depended on malicious code. (Proofpoint, 2016) The following are key findings of that report that show how social engineering has become popular in cyber security.

1. People are replacing automated exploits as attackers' preferred entry tactic

By an overwhelming margin, attackers infected computers by tricking people into doing it themselves, not through automated exploits. A whopping 99.7% of documents used in attachment-based campaigns relied on social engineering and macros. At the same time, 98% of URLs in malicious messages link to hosted malware, either as an executable or an executable inside an archive. To work, these files have to be opened by the user. So attackers trick users into double-clicking them and infecting themselves.

2. Dridex banking Trojan campaigns were the dominant technique for making people central to the infection chain

Stroud defines Dridex as a strain of banking malware that leverages macros in Microsoft Office to infect systems. Once a computer has been infected, Dridex attackers can steal banking credentials and other personal information on the system to gain access to the financial records of a user. (Stroud, 2016)

Banking Trojans were the most popular type of malicious document attachment payload, accounting for 74% of all payloads.

Dridex-based email volume was almost 10 times greater than the next most-used payload in such attacks. The document files in these messages contained malicious macros that tricked the recipient into running code to infect their computer. Employees' inboxes continued to be the primary way banking Trojans gain entry into your organization. Attackers use social engineering and mimicking familiar processes like invoices and statements to trick a user into clicking on the messages in their email. With social engineering, these messages may be even appear to be coming from a colleague or manager.

3. Attackers timed email and social media campaigns to align with the times that people are most engaged

As they shifted from malware exploits to clicks by humans, attackers optimized campaign delivery times to match the times when people click. Email messages are delivered at the start of the business day (9-10 a.m.) in the target regions. Social media spam posting times likewise mirror the peak usage times for legitimate social media activity. Even so, there was no time of day or day of week when malicious content was not being sent to people—or being clicked by them.

4. People willingly downloaded more than 2 billion mobile apps that steal their personal data

Attackers used social media threats and mobile apps, not just email, to trick users into infecting their own systems. One in five clicks on malicious URLs occurred off the network, many of them from social media and mobile devices. Malicious mobile apps are no longer corner cases—they're real-world threats. An analysis of authorized Android app stores discovered more than 12,000 malicious mobile apps— capable of stealing information, creating backdoors, and other functions—accounting for more than 2 billion downloads.

5. URLs linking to credential-phishing pages were almost three times more common than links to pages hosting malware

On average, 74% of URLs used in email-based attacks linked to credential-phishing pages, rather than to sites hosting malware. In email phishing campaigns, the attackers link to pages designed to entice people to provide their logins and other personal information. In effect, the victim does the work of keyloggers, infostealers, and other automated malware.

6. Accounts used to share files and images – such as Google Drive, Adobe, and Dropbox– are the most effective lures for credential theft

Google Drive links were the most clicked credential-phishing lures. Phishing emails that use these brands are more likely to succeed at tricking the user into clicking, especially if the victim receives the message from someone in their contacts list. These brand lures are effective because these services are familiar, and the user is used to clicking to sign in to view shared content.

7. Phishing is 10 times more common than malware in social media posts

The fastest growing social media threat was fraudulent customer-service account phishing, which uses social engineering to trick users to divulge logins and personal information. The ease of creating fraudulent social media accounts for known brands drives a clear preference for phishing in social media-based attacks. Distinguishing fraudulent social media accounts from legitimate ones is difficult: it was found that 40% of Facebook accounts and 20% of Twitter accounts claiming to represent a Fortune 100 brand are unauthorized. For Fortune 100 companies, unauthorized accounts on Facebook and Twitter make up 55% and 25% of accounts, respectively.

8. Dangerous mobile apps from rogue marketplaces affect two in five enterprises

The researchers identified rogue app stores that allowed users to download malicious apps onto iOS devices – even those not "jailbroken," or configured to run apps not offered through Apple's iTunes store. Lured in by "free" clones of popular games and banned apps, users who download apps from rogue marketplaces—and bypass multiple security warnings in the process are four times more likely to download an app that is malicious. These apps can steal personal information, passwords, and data. About 40% of large enterprises sampled by Proofpoint TAP Mobile Defense researchers had malicious apps from DarkSideLoader marketplaces—that is, rogue app stores—on them.

9. Low-volume campaigns of highly targeted phishing emails focused on one or two people within an organization to transfer funds directly to attackers

Highly targeted phishing messages to people with access to wire transfers hit organizations of every size across all industries.

Often called "wire transfer phishing" or "CEO Phishing," these Business Email Compromise (BEC) scams involve deep background research by the attackers. The emails have spoofed senders so they appear to be from the CEO, CFO, or other executive; they rarely have links or attachments; and they include urgent instructions to the recipient to transfer funds to a designated account (Proofpoint, 2016).

2.11 Various ERM Frameworks

The most popular ERM frameworks in use today are ISO 31000:2009 and COSO ERM.

ISO 31000:2009, Risk Management-Principles and guidelines

ISO 31000:2009, *Risk management – Principles and guidelines*, provides principles, framework and a process for managing risk. It can be used by any organization regardless of its size, activity or sector. Using ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment. However, ISO 31000 cannot be used for certification purposes, but does provide guidance for internal or external audit programmes. Organizations using it can compare their risk management practices with an internationally recognized benchmark, providing sound principles for effective management and corporate governance (ISO, n.d.).

COSO ERM Integrated Framework

In response to a need for principles-based guidance to help entities design and implement effective enterprise-wide approaches to risk management, COSO issued the *Enterprise Risk Management – Integrated Framework* in 2004. This framework defines essential enterprise risk management components, discusses key ERM principles and concepts, suggests a common ERM language, and provides clear direction and guidance for enterprise risk management. The guidance introduces an enterprise-wide approach to risk management as well as concepts such as: risk appetite, risk tolerance, portfolio view. This framework is now being used by organizations around the world to design and implement effective ERM processes. (COSO, n.d.)

Table 2 below summarizes the components of both frameworks.

Key Term or Description	**ISO 31000:2009**	**COSO ERM Framework**
Scope.	This International Standard provides principles and generic guidelines on risk management… it can be used by any public, private or community enterprise, association, group or individual. Therefore, this International Standard is not specific to any industry or sector.	This definition (of ERM) is purposefully broad. It captures key concepts fundamental to how companies and other organizations manage risk, providing a basis for application across organizations, industries and sectors. It focuses directly on achievement of objectives established by a particular entity and provides a basis for defining enterprise risk management effectiveness.
Risk management, defined.	Coordinated activities to direct and control an organization with regard to risk.	Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.
Risk, defined.	The effect of uncertainty upon objectives.	The possibility that an event will occur and adversely affect the achievement of objectives.
Risk appetite, defined.	The amount and type of risk that an organization is willing to pursue or retain.	A broad amount of risk an entity is willing to accept in pursuit of its mission or vision.
Risk assessment, defined.	The overall process of risk identification, risk analysis and risk evaluation.	Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risk are assessed on an inherent and a residual basis.

Risk management process	Continually and interactively: Communicate and consult • Establish the context • Risk assessment: o Identification o Analysis o Evaluation • Risk treatment Continually & iteratively: Monitor and review	• Internal environment • Objective setting • Event identification • Risk assessment • Risk response • Control activities • Info & communication • Monitoring

Table 2: ISO 31000 & COSO ERM

Why COSO ERM?

1. COSO is much stronger in the concepts of alignment of risk with strategy, which is critical to a holistic methodology. The fact that it is complicated is a hollow argument. Risk Management isn't supposed to be simple.
2. The principles are easy to understand and the linkage of the objectives to the components of the risk management
3. ISO 31000 does not deal adequately with risk assessment and risk appetite.
4. COSO ERM defines organizational structure with the 5 components of internal control but expands on the risk assessment component to address risk identification, etc. COSO ERM also doesn't prescribe exact requirements but instead uses a principles based orientation and outlines the characteristics or attributes of ERM most organization types can follow and apply to their own unique circumstances.
5. COSO has been tested over time and its applicability to many industries is well proven
6. It is proactive and not reactive. This is because it factors in the possibility that an event will occur and adversely affect the achievement of objectives.
7. Stronger on corporate governance aspects. Allows direct delivery of expectations from Board and Top Management related to CG legal obligations.
8. Applied across the enterprise, at every level and unit.

2.12 THE COSO ERM Framework

COSO's enterprise risk management (ERM) model has become a widely-accepted framework for organizations to use. Although it has attracted criticisms, the framework has been established as a model that can be used in different environments worldwide.

COSO's guidance illustrated the ERM model in the form of a cube. COSO intended the cube to illustrate the links between objectives that are shown on the top and the five components shown

on the front, which represent what is needed to achieve the objectives. The third dimension represents the organization's units, which portrays the model's ability to focus on parts of the organization as well as the whole.

The COSO Cube

(Galligan & Rau, 2015)

Figure 1: The COSO Cube

Internal Control Components and Related Principles

The following is a summary of the 17 internal control principles by internal control components as presented in the *2013 Framework.*

Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring Activities
1. Demonstrates commitment to integrity and ethical values **2.** Exercises oversight responsibilities **3.** Establishes structure, authority, and responsibility **4.** Demonstrates commitment to competence **5.** Enforces Accountability	**6.** Specifies suitable objectives **7.** Identifies and analyses risk **8.** Assesses fraud risk **9.** Identifies and analyses significant change	**10.** Selects and develops control activities **11.** Selects and develops general controls over technology **12.** Deploys through policies and procedures	**13.** Uses relevant, quality information **14.** Communicates internally **15.** Communicates externally	**16.** Conducts ongoing and/or separate evaluations **17.** Evaluates and communicates deficiencies

Table 3: Internal Controls and Related Principles

The underlying premise of enterprise risk management is that every entity exists to provide value for its stakeholders. All entities face uncertainty, and the challenge for management is to determine how much uncertainty to accept as it strives to grow stakeholder value.

Uncertainty presents both risk and opportunity, with the potential to erode or enhance value.

Enterprise risk management enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value.

Value is maximized when management sets strategy and objectives to strike an optimal balance between growth and return goals and related risks, and efficiently and effectively deploys resources in pursuit of the entity's objectives. Enterprise risk management encompasses:

Aligning risk appetite and strategy – Management considers the entity's risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.

Enhancing risk response decisions – Enterprise risk management provides the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance.

Reducing operational surprises and losses – Entities gain enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses.

Identifying and managing multiple and cross-enterprise risks – Every enterprise faces a myriad of risks affecting different parts of the organization, and enterprise risk management facilitates effective response to the interrelated impacts, and integrated responses to multiple risks.

Seizing opportunities – By considering a full range of potential events, management is positioned to identify and proactively realize opportunities.

Improving deployment of capital – Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.

These capabilities inherent in enterprise risk management help management achieve the entity's performance and profitability targets and prevent loss of resources. Enterprise risk management helps ensure effective reporting and compliance with laws and regulations, and helps avoid damage to the entity's reputation and associated consequences. In sum, enterprise risk management helps an entity get to where it wants to go and avoid pitfalls and surprises along the way.

2.13 Conceptual Framework

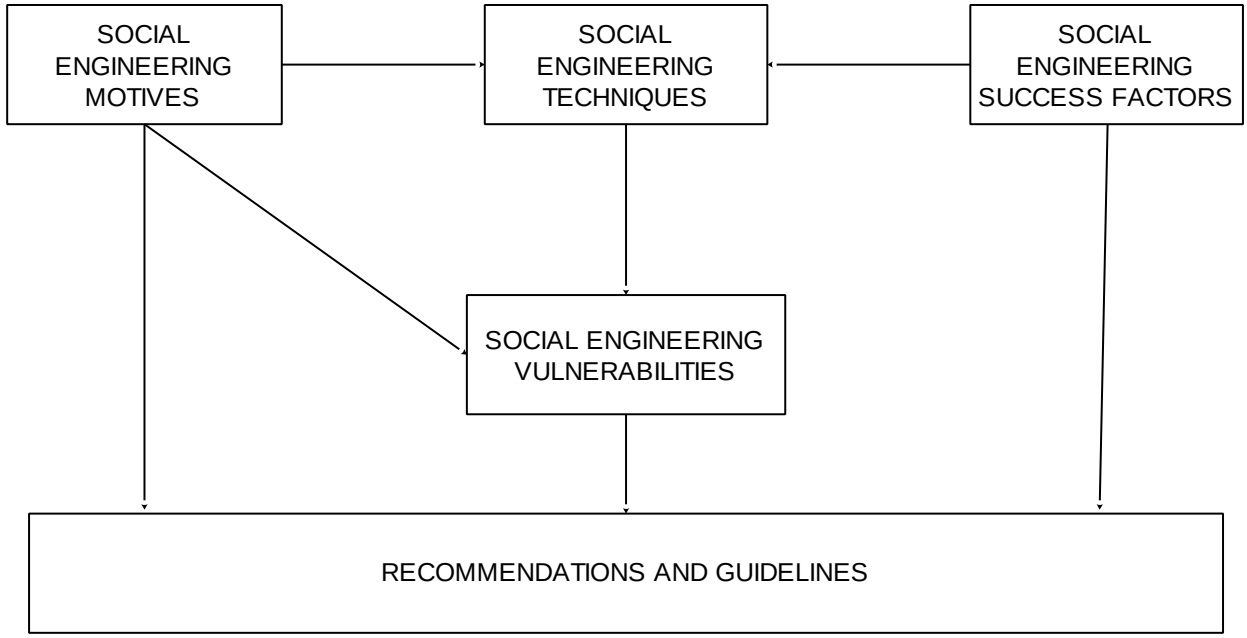


Figure 2: Conceptual Framework

1. Motives-these are factors that influence the decision of a social engineer to carry out an attack.
2. Techniques- these are the skills an attacker employs when carrying out his/her attack. The techniques used will be highly influenced by the motive(s) of the attacker.
3. Success Factors- elements that a social engineer may look for or exploit in a target when attempting an attack. These factors tend to enhance the technique in use e.g. the trait of agreeableness in a potential target may play a big role in the success of a Pretext/role playing attack.
4. Vulnerabilities-this is the effect or result realized after a social engineer successfully carries out an attack on a target. The scale/magnitude may differ depending on the motive of the social engineer. If the motive of the attack was financial gain, the result would be financial losses. The success level of the technique will also influence the scale/magnitude of the attack.
5. Recommendations and Guidelines-Recommendations aid in countering the threat of social engineering in its entirety while the guidelines will be used to manage the risk brought about by social engineering attacks in accordance to the organization's risk appetite.

2.14 Summary of the studies

The following studies have been carried out in the past in an attempt to counter the threat of social engineering.

Gaining Access with Social Engineering: An Empirical Study of the Threat

Michael Workman (Workman, 2007) lays emphasis on the social engineering victim's psychological traits that may lead to successful exploitation. The study focuses on social engineering as a whole touching on methodologies of social engineering, aspects that influence successful attacks and also give guidelines on how to reduce its threat in the organization. The psychological traits will only be dealt with at a high level.

Social Engineering Your Employees to Information Security

Manjak (Manjak, 2006) examines the role and value of Information Security Awareness efforts in the organization. It discusses the various threats (e.g., social engineering tactics) targeting employees that an InfoSec Awareness campaign is designed to counter. It also reviews some of the obstacles to implementing a program, offer some tools and strategies for developing effective materials. The main focus here is not on the human element but on the value that InfoSec Awareness campaigns bring to the organization.

The study highlights what role the human element has to play in ensuring information security. This was after examining the threats posed by Social Engineering and the impact they may have in the organization if successfully implemented.

Social Engineering: A means to violate a computer system

Allen's (Allen, 2006) paper acts as a guide on the subject of Social Engineering and explains how it might be used as a means to violate a computer system(s) and/or compromise data. Topics touched on include: Definition(s) of social engineering, the cycle of a social engineering attack, Human behavior (from both sides of the fence) and Counter-measures.

The main focus area of this paper is the security experts as it gives recommendations on what they are to do to ensure social engineering threats are thwarted.

This study brings all the stakeholders i.e. Policy makers, Security experts and Users on board in ensuring that the social engineering threat is countered. This approach will ensure acceptance across the board in the organization as each stakeholder will have a clear cut role when it comes to security of the organization's information and assets.

CHAPTER 3-METHODOLOGY

3.1 Introduction

This section highlights the various methods and procedures that were adopted in conducting the study in order to meet its objectives and answer the research questions.

3.2 Research design

A detailed outline of how an investigation will take place. A research design will typically include how data is to be collected, what instruments will be employed, how the instruments will be used and the intended means for analyzing data collected. (Business Dictionary, n.d.)

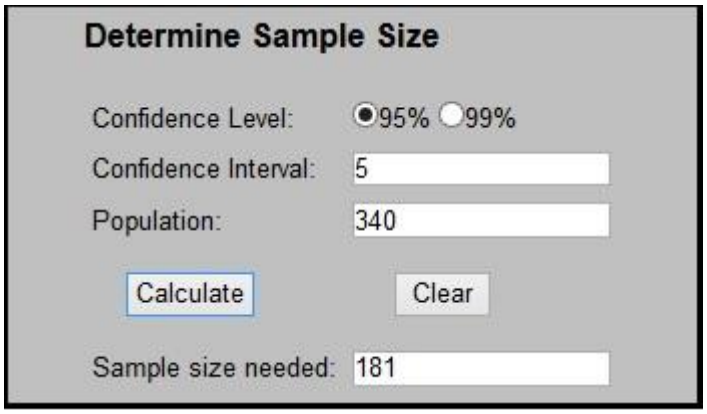
This study adopted a hybrid of quantitative and qualitative methodologies.

3.3 Target population

A particular group of people that is identified as the intended recipient of an advertisement, product, or campaign. Also called target audience. (Business Dictionary, n.d.)

This study targeted the stakeholders of a general insurance company whose headquarters are situated in Nairobi and they can be generally categorized as Policy makers, Security Experts (IT Department in this case) and the Users themselves.

The company has a workforce of about 340 personnel both permanent and temporary. An online sample calculator was used to determine how many respondents would be needed during the questionnaire distribution in order to get results that reflect the target population as precisely as needed.



(Creative Research Systems, 2015)

Figure 3: Determine Sample Size

Thus the researcher settled for distribution of 180 questionnaires.

3.4 Research instruments

The study being descriptive was observational and also made use of questionnaires. Nebeker (Nebeker, n.d.) defines a descriptive study as one in which information is collected without changing the environment (i.e., nothing is manipulated). Sometimes these are referred to as "correlational" or "observational" studies.

This observational study explored various social engineering techniques i.e. Shoulder Surfing, Dumpster Diving, Pretext/Role Playing and also Surfing the Organizational Website and Social Pages (Social Network Squatting). The results of the study were used to determine areas and departments in the organization that posed the highest security risk in the organization and need to be improved. Study results were also used to calculate a risk score or the probability of compromise or breach involving stakeholders in the organization.

A survey consists of a predetermined set of questions that is given to a sample. With a representative sample, that is, one that is representative of the larger population of interest, one can describe the attitudes of the population from which the sample was drawn. A good sample selection is key as it allows one to generalize the findings from the sample to the population, which is the whole purpose of survey research. (Shaughnessy, et al., 2012, pp. 140-145)

This "Security Awareness Survey" was designed to ask stakeholders how they would respond to specific security related questions and situations. The results of this survey were used to calculate a risk score, or the probability of compromise or breach involving employess. The generated score and risk level can be tracked over time as metric to measure program goals and initiatives, or it can also be used to compare with industry peers.

3.5 Data collection procedure

The primary data collection methods was through observation and survey by use of questionnaires. The study incorporated observation on the various stakeholders in the organization as they went about their routine activities around the workplace. It was carried out within the confines of the organization's offices. Where necessary as in the case of pretext/role playing an outsider was used so as to ensure data obtained would be authentic and free from any bias. It is also important to note that there was no prior knowledge among the stakeholders as this exercise was being carried out to ensure integrity and authenticity of the data obtained.

The questionnaires contained closed ended questions which were distributed to the respondents as hard copies. The questionnaires were distributed through an appointed person in each department and branch which made it easier for collection once the respondents were done.

3.6 Data analysis procedure

After the data collection exercise was complete, the questionnaires were analyzed to check for errors, completeness. The results of the tests were compiled at the end of the tests. The data from the questionnaires was subjected to a risk level matrix. The risk levels ranged from 1-5 where 1 is for Low Risk and 5 for High Risk.

The data collected from the observation was classified by the number of 'successful hits' and also ranked by the risk level of each department/branch depending on the sensitivity of data that they handle e.g. Finance Department may have a higher risk ranking as compared to the Underwriting Department.

The collected data was coded and entered into the Statistical Package for Social Sciences (SPSS). SPSS was used because it aids in organizing and summarizing the data to provide meaningful parameters, which are useful for data analysis, which include measures of, frequency distribution, percentages, correlation and regression analysis, frequencies, means, standard deviation and percentages, especially from quantitative data.

CHAPTER 4-DATA ANALYSIS, RESULTS AND DISCUSSION

4.1 Introduction

This chapter is a presentation of results and findings obtained from field responses by use of observation methods and questionnaires. The collected data is broken into two sections. The first section deals with the background information, while the other section presents findings of the analysis, based on the objectives of the study as explored by the questionnaires where both descriptive and inferential statistics have been employed.

4.2 Response Rate

It was noted from the data collected, out of the 180 questionnaires administered to the employees at the insurance company, 150 questionnaires were filled and returned. This represented an 80% response rate, which is considered satisfactory to make conclusions for the study. According to Mugenda and Mugenda (Mugenda & Mugenda, 2003) a 50% response rate is adequate, 60% good and above 70% rated very good. This also collaborates Bailey (Bailey, 1987)) assertion that a response rate of 50% is adequate, while a response rate greater than 70% is very good. This implies that based on this assertion; the response rate which was calculated in this case according to Mugenda and Mugenda and Bailey was very good.

This high response rate can be attributed to the data collection procedures, where the researcher pre-notified the potential participants and applied the drop and pick method where the questionnaires were picked at a later date to allow the respondents ample time to fill the questionnaires.

4.3 Pilot Test

To establish validity, the research instrument was given to experts who were experienced to evaluate the relevance of each item in the instrument in relation to the objectives. The same were rated on the scale of 1 (very relevant) to 4 (not very relevant). Validity was determined by use of content validity index (CVI). CVI was obtained by adding up the items rated 3 and 4 by the experts and dividing this sum by the total number of items in the questionnaire. A CVI of 0.894 was obtained. Oso and Onen (Oso & Onen, 2009), state that a validity coefficient of at least 0.70 is acceptable as a valid research hence the adoption of the research instrument as valid for this study. The questionnaires used had Likert scale items that were to be responded to. For reliability analysis Cronbach's alpha was calculated by application of SPSS. The value of the alpha coefficient ranges from 0 to 1 and may be used to describe the reliability of factors extracted from dichotomous (that is, questions with two possible answers) and/or multi-point formatted questionnaires or scales (i.e., rating scale: 1 = poor, 4 = excellent). A higher value shows a more reliable generated scale. Cooper

& Schindler indicated 0.7 to be an acceptable reliability coefficient (Cooper, & Schindler, 2008). Since, the alpha coefficients were all greater than 0.7, a conclusion was drawn that the instruments had an acceptable reliability coefficient and were appropriate for the study.

4.4 Descriptive statistics

Descriptive statistics are sometimes called inductive statistics. These are facts and figures sifted and arranged in a manner that enables the researcher to understand the nature of the population he/she is studying. This kind of statistics brings out the quality of the data under examination through simplification. The study sought to establish the descriptive statistics of the responses from the respondents. The results of the findings are illustrated in the following subsections.

Demographic Information-Illustrates the respondents' position within the organization

Anti-viruses and Firewalls. To assess the respondents' knowledge in regards to anti-viruses and firewalls.

Emails. To assess the respondents' knowledge on Emails and how to identify scams sent through emails.

Policies and Passwords. To assess respondents' knowledge to organization policies and password fundamentals.

General Security Questions to assess respondents' knowledge in regards to information security in general and best practices.

4.4.1 Position within the organization

The study sought to determine the positions the respondents held in the firm. From the analysis of the findings, it was noted that majority of the respondents were full time employees in the organization. This was indicated by the frequency of 99 respondents who stated this and was calculated to amount to 66% of the total respondents. This was closely followed by respondents who stated that they worked as part time employees in the firm with a frequency of 45 respondents which amounted to 30% of the respondents. Only 6 (4%) of the respondents stated that they were interns at the insurance company. Therefore it was clear that majority of the respondents were either full time or part time employees at the firm and were therefore in a good position to provide the information needed to meet the objectives of the study.

4.4.2 Existence of an Information security team

The study also sought to determine whether the organization had an information security team.

From the SPSS analysis, it was noted that majority of the respondents indicated that their organization did not have a security team. This was indicated by 116 (77%) of the total respondents, only a mere 34 (23%) of the respondents stated that the organization had an

information security team. From the findings, it was clear that it was necessary for one to be formed or if it exists it should be properly commuinacted of its existence.

4.4.3 Detection and contact in case of security threats

The study sought to determine whether the respondents would be able to detect any security threat. The results of the findings are illustrated in figure 7.

From the analysis of the findings it was noted that majority of the respondents(71.5%) indicated that there was a security threat, they would know what to look for. Closely after were respondents (22%) who stated that in case of a security threat they would not know what to look for. Only 6.5% of the respondents that incase there was a security threat they were not sure they would know what to look for.

Of the responses, 88 (56%) indicated that they did not know who to contact in case they were faced with an information security threat. And 66 (44%) of the respondents stated that they knew who to contact when faced with an information security threat.

From the analysis of the findings it was noted that majority of the respondents 125 (83%) indicated that their computers had been infected before. Only 17 (11%) of the respondents in the study indicated that their computer had not been infected before. A mere 8 (6%) of the respondents indicated they did not know what a virus or Trojan was. It was therefore evident from the study that majority of the respondents knew what a virus/Trojan is and had been previously infected by either of those.

4.4.4 Effects in relation to emails

The study sought to establish whether the respondents, once they received mail they would rely on the fact that it comes from the person in the "From" address.

From the analysis of the findings, it was noted that 68 (45%) of the respondents indicated that they could rely on the fact that the email comes from the person in the address. Closely following was 50 (33%) of the respondents stated that they could not rely on the fact that the email comes from the person in the "From" address. 32 (22%) of the respondents indicated that they did not know if they could rely on the fact that the email came from the person indicated in the from address.

From the analysis of the findings it was noted that majority of the respondents 100 (67%) indicated that they did not know how to identify an email scam while only a mere 50 (33%) indicated that they knew how to identify an email scam.

4.4.5 Effects in relation to antiviruses

The study sought to determine if an anti-virus was currently installed, updated and enabled on the respondents' computer. The results from the analysis are illustrated in Figure 12.

From the analysis of the findings, it was noted that majority of the respondents (44%) indicated that an antivirus was not installed in their computers. This was calculated from a frequency of 66 respondents and was closely followed by a frequency of 50 (33.3%) respondents who stated that their computers were installed with an antivirus. 24 (16%) of the respondents that they did not know how to tell while 6.5% indicated that they did not even know what an antivirus is.

4.4.6 Policies on the websites which employees can visit

The study also sought to determine whether the respondents knew of policies on websites which employees can visit.

From the analysis of the findings, it was noted that majority of the respondents indicated that there were policies, limiting what websites they could or could not visit while at work but they did not know of the policies. This was calculated from a frequency of 78 respondents who stated this. This was calculated to amount to 52% of the total respondents. Closely after were respondents 34 (22.7%) who stated that the organization had no policies and they could visit whatever website they wanted while they were at work. 38 (25.3%) of respondents stated that their branches had policies governing the websites to visit and that they knew and understood them.

4.4.7 Largest source of risk to your department's information security

The study sought to establish the largest source of risk to the department's information security.

From the analysis of the findings, it was established that majority of the respondents (42.5%) indicated that their largest source of risk in their department was defective software. This was calculated from a frequency of 85 respondents. This was closely followed by respondents who indicated that the largest source of risk in their department was computer viruses and other "malware" with a frequency of 56 respondents which amounted to 28% of the total respondents. 45 (22.5%) of the respondents indicated that human mistakes, malicious or otherwise were the largest source of risk to the department information security while 14 (7%) blamed it on Defective hardware.

4.4.8 Ways that you can secure your password from disclosure

The study also sought to establish ways in which the respondents thought they could secure their passwords from disclosure.

From the analysis of the findings, it was noted that majority of the respondents (59.3%) indicated that they could write down on a sticky pad and stick it in their computers. This was calculated from a frequency of 89 respondents. Closely after were respondents (24%) who stated that they could write down the password if they could keep it in a secure place like their wallets without header information. This was calculated from a frequency of 36 respondents. 21 (14%) of the respondents indicated that they saved their passwords on their phones for quick access. The least

frequency was of respondents 4 (2.7) who stated that all the mentioned methods were applicable in securing their passwords from disclosure.

4.5 Response on various statements.

Descriptive Statistics					
	N	**Minimum**	**Maximum**	**Mean**	**Std. Deviation**
Do you know who to contact in case of an IT security incidence	150	1.00	2.00	1.0667	.25028
Have you ever found a virus or Trojan on your computer at work	150	1.00	3.00	1.7467	.66743
In what situations have you ever given your password from work to someone else	150	1.00	3.00	2.2800	.87562
If you format a harddrive/flashdisk or erase the files on it all the information on it is permanently lost	150	1.00	3.00	1.8533	.81419
Who is responsible for information security in your department	150	2.00	3.00	2.5200	.50127
Is there firewall in your computer	150	1.00	3.00	1.6000	.91959
Is your computer configured to be automatically updated	150	1.00	3.00	1.5000	.67307
You recieve an attachment which does not appear related to work and it is received from someone you do not know:	150	1.00	4.00	3.1000	1.04753
Do you know what an email is and how to identify one	150	1.00	2.00	1.7000	.45979
The links in emails from unfamiliar sources are generally safe to click on	150	2.00	2.00	2.0000	.00000
Do we have policies on how you can or cannot use emails	150	2.00	3.00	2.1000	.30101
Is an instant messaging allowed in our organization	150	1.00	3.00	2.0000	.43350
Can you own a personal device, to store and transfer company information	150	1.00	4.00	1.9267	.81180
When constructing you should	150	1.00	4.00	3.0000	1.26915
Do you use the same password for your work accounts as you do for your personalaccount at home, such as facebook, Twitter or your personal email account	150	1.00	2.00	1.9133	.28229
How often do you take information from the office and use your computer at home to work on it?	150	3.00	4.00	3.8733	.33371
Have you logged into work account using public computers, such as from a library, cyber cafe or mail	150	2.00	2.00	2.0000	.00000

Have you received an email, call or sms within the past 6 months that you suspect was an attempt to get your personal email by fraudulent purpose	150	1.00	2.00	1.7333	.44370
Do you have a method to validate your bank or mobile phone sevice provider when they call/text e.g M-pesa	150	1.00	3.00	1.6000	.66555
How do you get rid of information such a bank statement	150	1.00	3.00	2.1000	.83345
Have you heard the term phishing before	150	1.00	2.00	1.9000	.30101
Have you heard term "Social engineering" before	150	1.00	2.00	1.4000	.49154
What do you think it means if you have answered "Yes" above	150	2.00	3.00	2.3000	.45979
You notice someone in the office you do not know.What do you do?	150	1.00	4.00	3.3867	.96785
Do you think it is necessary to call a company to verify the identity of its employee if presented with an ID card	150	1.00	2.00	1.2667	.44370
What is one of the ways that you can secure your pasword from disclosure	150	2.00	4.00	2.3600	.63753
My email is private and no one can look at it	150	1.00	2.00	1.1733	.37980
Valid N (listwise)	150				

Table 4: Response on various statements.

From the findings in the SPSS analysis, it was noted that majority of the respondents indicated that incase of an IT security incident they would know who to contact. This was noted by the mean calculated of 1.0667. The standard deviation calculated indicated uniformity in the responses from the respondents.

The study also established that most of the respondents stated that their computers had been infected by a virus or trojan in their work place. This was noted true by the mean calculated in the SPSS of 1.7467. The standard deviation calculated of 0.66743 indicated little variation in the responses.

From the findings it was inferred that majority of the respondents had never given their password from work to someone else. This was supported by the mean calculated of 2.28, the standard deviation indicated uniformity in the responses from the respondents. The study also noted that majority of the respondents indicated that if the hard disk is formated or erased all the files and information is not completely lost. This was noted true by the mean calculated of 1.8533 which when rounded off represented false.The standard deviation calculated of 0 .81419 indicated uniformity in the responses from the respondents.

The study also established that the local IT support staff were responsible for information security in their department. This was noted true by the mean calculated in the analysis of 2.5200 and the standard deviation calculated of 0.5 implied that majority of the respondents stated that everyone

was responsible for information security in their department or it was the responsibility of the local IT support staff

The study also sought to determine whether there was a firewall in the respondents computers. From the analysis of the findings, it was noted that majority of the respondents indicated that a firewall was not enabled in their computers. This was noted by the mean calculated in the SPSS analysis of 1.6, The standard deviation indicated that majority of the respondents were of a similar opinion.

The study also sought to establish whether the respondents' computers had been configured to be automatically updated. From the findings in the analysis, majority of the respondents indicated that their computers were not automatically updated. This was determined by the mean calculated of 1.5 and a standard deviation of .67307. The standard deviation calculated indicated uniformity in the responses from the respondents.

The study also noted from the SPSS analysis that majority of the respondents indicated that they read the email, but do not open any attachment unless they know the sender in case they recieve an attachment which does not appear related to work and it is received from someone you do not know. This was noted by the mean calculated of 3.1000. The standard deviation indicated uniformity in the responses from the respondents

From the analysis, it was established that majority of the respondents did not know what an email scam was and also didnt know how to identify one. This was noted tru by the mean calculated of 1.7000. The small standard deviation calculated of 0.4 indiated uniformity in the responses from the respondents. From the findings it was also established that The links in emails from unfamiliar sources are not generally safe to click on. This inference was established by the mean calculated in the analysis of 2.0000. The standard deviation calculated of 0.000 indicated that none of the respondents indicated otherwise.

The study establsihed also that there were policies limiting what websites that the respondents could visit as noted by the mean calculated in the analysis of 2.1000. The standard deviation calculated in the analysis indicated uniformity in the reponses. The study also noted that majority of the respondents indicated that instant messaging was not allowed in their organization. This was noted true by the mean calculated in the analysis of 2.0. The small standard deviation calculated in the analysis indicated uniformity in the reponses from the repondents.

From the analysis, it was established that majority of the respondents indicated that they did not use the same password for their work accounts as they did for your personalaccount at home, such as facebook, Twitter or their personal email account. This was noted true by the mean calculated in the analysis of 1.9133. The study also noted that majoriy of the respondents indicated that they never took information from the office and use their computer at home to work on it. This was

noted true by the mean calculated of 3.8733. The standard deviation calculated indicated that majority of the respondents were of a similar opinion.

From the findings, the study noted that majority of the respondents indicated that incase they noticed someone in the office that they did not know, they would leave them alone if the person doesnt apear lost and if they needed help the would ask. This was noted true by the mean calculated in the analysis of 3.3867. The study also noted that one of the ways the can secure their passwords from disclosure would be to write it down only if they can keep it in a secure place like their wallets without header information. Majority of the respondents also indicated that their emails were secure and no one could look at them.

Generally it was noted that majority of the respondents were ignorant of the computer threats faced or those that they might encounter and hence there was need to manage the human element of security in the organization.

4.6 Security Awareness Survey

This "Security Awareness Survey" was designed to ask stakeholders how they would respond to specific security related questions and situations. The results of this survey were used to calculate a risk score, or the probability of compromise or breach involving employess. The generated score and risk level can be tracked over time as metric to measure program goals and initiatives, or it can also be used to compare with industry peers.

This survey consists of 34 questions. Some of the question responses in this survey indicate strong awareness and good security practices while others indicate weak awareness, negligent behavior, or high-risk activities. Based on these differences, each question response in this survey (except for the first question) has been assigned a risk value (1-5). "One" is the lowest risk value and "five" is the highest risk value. When the results of the survey were collected, they were used to determine the overall risk score or risk level of the organization. The results of the risk analysis are illustrated in Table 5 below.

Question	Frequency	Risk value	Response total
Do you know who to contact in case of an IT security incidence	140	4	560
Have you ever found a virus or Trojan on your computer at work	74	3	222
In what situations have you ever given your password from work to someone else	84	4	336
If you format a harddrive/flashdisk or erase	88	4	352

the files on it all the information on it is permanently lost			
Who is responsible for information security in your department	78	3	234
Is there firewall in your computer	105	4	420
Is your computer configured to be automatically updated	90	3	270
You recieve an attachment which does not appear related to work and it is received from someone you do not know: Do you	75	3	225
Do you know what an email is and how to identify one	105	4	420
The links in emails from unfamiliar sources are generally safe to click on	105	4	420
Do we have policies on how you can or cannot use emails	135	4	540
Is an instant messaging allowed in our organization	76	3	228
Can you own a personal device, to store and transfer company information	84	3	252
When constructing you should	90	3	270
Do you use the same password for your work accounts as you do for your personalaccount at home, such as facebook, Twitter or your personal email account	76	3	228
How often do you take information from the office and use your computer at home to work on it?	131	4	524
Have you logged into work account using public computers, such as from a library, cyber cafe or mail	34	2	68
Have you received an email, call or sms within the past 6	150	5	750

months that you suspect was an attempt to get your personal email by fraudulent purpose			
Do you have a method to validate your bank or mobile phone sevice provider when they call/text e.g M-pesa	75	2	150
How do you get rid of information such a bank statement	65	2	130
Have you heard the term phishing before	135	4	540
Have you heard term "Social engineering" before	90	3	270
What do you think it means if you have answered "Yes" above	105	4	420
You notice someone in the office you do not know.What do you do?	97	4	388
Do you think it is necessary to call a company to verify the identity of its employee if presented with an ID card	110	4	440
What is one of the ways that you can secure your pasword from disclosure	107	4	428
My email is private and no one can look at it	124	4	496

Table 5: Risk Analysis

1. For each of the 34 questions, multiply each question response risk value (1-5) by the number of times it was choosen by the survey takers.

   <response risk value> X <the number of times choosen> = <response total>
2. Add up all of the response totals for a survey cumulative response total.
3. Divide the survey cumulative response total by the number of survey takers to calculate the Survey (or organization's) risk score.

   <cumulative response total> / <number of survey takers> = Organization's Risk Score
4. Using the risk score, check the "Risk Levels" table below for the organization's general risk rating

Risk Levels

	Risk Levels	Description
1	Low (25 – 39)	Users are aware of good security principles and threats, have been properly trained, and comply with all organizational security standards and policies.
2	Elevated (40 – 60)	Users have already been trained on organizational security standards and policies, they are aware of threats, but may not follow good security principles and controls.
3	Moderate (61 – 81)	Users are aware of threats and know they should follow good security principles and controls, but need training on organizational security standards and policies. They also may not know how to identify or report a security event.
4	Significant (82 – 96)	Users are not aware of good security principles or threats nor are they aware of or compliant with organizational security standards and policies.
5	High (97 – 110)	Users are not aware of threats and disregard known security standards and policies or do not comply. They engage in activities or practices that are easily attacked and exploited.

Table 6: Risk Level and Description

The research sought to establish the risk levels through security risk awareness. From the findings the following risks were established as shown in the table above. The cumulative risk score was established by dividing the survey cumulative response total by the number of survey takers to calculate the survey (or organization's) risk score. The models risk score was calculated to **63.87** which indicated that users are aware of threats and know they should follow good security principles and controls but need training on organizational security standards and policies. They also may need to know how to identify and report a security threat.

4.7 An analysis from the test of the social engineering techniques

Rank	Classification	Impact
4	**Highly Sensitive:**	Highly sensitive data is defined as "Information that if disclosed or modified without authorization would have severe adverse effect on the operations, assets, or reputation of the Organization, or the Organization's obligations concerning information privacy." This includes, but is not limited to, online banking portal logins, payroll information and staff health insurance data. Highly Sensitive Data may not be shared.
3	**Sensitive:**	Sensitive data is defined as "Information that if disclosed or modified without authorization would have serious adverse effect on the operations, assets, or reputation of the Organization, or the Organization's obligations concerning information privacy." This includes, but is not limited to, contract details covered by Non-Disclosure Agreements.
2	**Internal:**	Internal Data is defined as "Information that if disclosed or modified without authorization would have moderate adverse effect on the operations, assets, or reputation of the Organization, or the Organization's obligations concerning information privacy." This includes, but is not limited to, information such as a client's claim experience. Internal Data can be shared with the owning unit, other units, other organizations, and the government as long as there is a legitimate and documented business need for said parties to see the data in question, but may not be shared with the media.
1	**Public:**	Information that is classified as public information can be freely shared with the public and posted on publicly viewable web pages. This includes but is not limited to branch networks and contacts.

Table 7: Data Ranking and classification Table (University of Illinois, n.d.)

The table above was used as a guide to rank and classify the data/information available in the various departments that are found in the organization.

4.7.1 Shoulder surfing

The study sought to observe the behavioral characteristics displayed by the users as they access the resources entrusted to them. This may include but not limited to banking portals and Personnel databases. This was to ascertain the department that would be most susceptible to vulnerabilities if an attack were to occur. The exercise was carried out at close range considering the targets are confined to an office setting. The social engineer randomly walked into the various departments in the organization more so during morning hours and after lunch when users log in to the various systems.

In order to establish the success factor of the technique, the number of successful 'hits' in trying to obtain data such as passwords was documented and classified by rank and department. The findings of the analysis are tabulated below for each department

	Rank	Successful hits
Claims	1	34
Human Resources Department	4	25
Underwriting	2	36
Finance	4	44

Table 8: Shoulder Surfing

From the findings, the highest number of successful hits was in the Finance department with a total of 44 hits. A hit in this case is the number of instances that the social engineer will succeed at obtaining information from an unsuspecting victim by way of shoulder surfing. 40 of the hits were when users were logging in to the Insurance ERP that the organization is using and 4 were when users were accessing online banking portals. Closely after was the Underwriting department with a total of 36 successful hits. 30 of the hits were during the logging into the Insurance ERP and the rest were when logging in to various valuators' portals. The Claims department had 34 successful hits while the Human Resource department was the most 'cautious' of the lot with 25 successful hits which were all from the insurance ERP.

The study noted that the Finance and Human Resources departments ranked highest in terms of sensitivity of the data that they handle, which would cause most damage if a social engineer managed to log in into, with a rank of 4. The Underwriting department was ranked second with 3 while the Claims department was ranked lowest in relation to the information held in their systems.

The high number of hits in the various departments can be attributed to the following.

The open office setting in the organization makes it easier for a social engineer to carry out his/her attacks without raising any suspicion. Cubicles should be introduced to enhance privacy and security.

The staff casually log in to the ERP without taking any precaution to protect their credentials making it easy for someone to decipher their passwords with minimal attempts. An awareness campaign on the security threat posed by not protecting their login credentials to the various systems should be conducted throughout the organization.

The high number of hits and sensitivity ranking of the Finance department means it poses the biggest threat in case an attack were to occur in the organization.

4.7.2 Dumpster diving

The aim of this exercise was to identify the department that would pose the biggest security threat in case of an attack in regards to how they dispose the information that is entrusted to them. The study determined the risk that each of these departments posed as a result of that technique.

The social engineer located and went through the trash bins that are placed in each department and retrieved as much as he/she can in regards to information that is classified as sensitive to the organization e.g. pay-slips in the case of the Human Resources department. The departments targeted were Finance, Underwriting and Human Resource.

	Rank	Successful hits
Human resource department	3	4
Finance	4	10
Underwriting	2	32

Table 9: Dumpster Diving

According to the findings of the analysis, it was noted that majority of the successful hits were from the Underwriting department with 32 hits. 20 of them were debit notes (A premium debit note or invoice indicates the premium charged by the insurer(s) for the insurance, the amount of any rebate or discounts to you and the net amount of premium payable to the insurance company), 5 were rating tables for the various insurance packages and 7 partly filled policy documents (The Policy/Certificate document sets out comprehensively the terms of the insurance and constitutes the definitive terms of any insurance cover) that contained vital information like clients' contacts, bank details and PIN numbers. This is due to the large volume of paperwork that they handle on a day to day basis. The Finance department was second with 10 successful hits. 5 being blank petty cash voucher slips, 3 bank statements and 2 partly filled cheques. The department with the least successful hits from dumpster diving was the Human resources department with only 4 successful hits. This can be attributed to the fact that most of their information is contained in systems. For this exercise hits are any information collected and classified according to its respective sensitivity ranking.

The Finance department was ranked highest at 4 and could again be classified as the riskiest department due to the nature of the data they handle off the ERP which can be classified as sensitive and highly sensitive.

The study thus saw the need to encourage vigilance in the disposal of information that may pose a threat to the organization especially in the Finance department. Immediate shredding or incineration of unwanted documents should be encouraged among the staff.

4.7.3 Surfing Organizational Website and Social Pages (Social Network Squatting)

The information gathered during this exercise was crucial in the lead up to the pretext/role playing exercise. This is because the social engineer was able to gather information such as but not limited to Branch Network, Board Members and Senior Management composition from the website. The social engineer was also able to get specific line manager's and personnel names and contacts from

queries made in the organization's social media pages. There was no ranking at this stage as it is considered a foot-printing phase where the social engineer gathers information that he/she gets to make use of later to make the pretext/ role playing look more authentic/realistic.

But this is not to say that this would not pose a risk to your organization depending on the information contained therein.

4.7.4 Pretexting/ Role playing

Pretexting is defined as the act of creating an invented scenario to persuade a targeted victim to release information or perform some action. It is more than just creating a lie, in some cases it can be creating a whole new identity and then using that identity to manipulate the receipt of information or access to a restricted place. (Social Engineer Inc, n.d.)

Therefore this study also sought to determine what branches are most vulnerable in terms of access thus posing as the biggest threat in regards of information security. A total of three branches were selected as targets due to the proximity they are from the head office and also the high number of human traffic in and out. An outsider was used for this exercise to ensure the information collected was authentic and free of bias. The pretext in this case was for the social engineer to pose as a CCTV technician who had come to carry out maintenance on the equipment in the branch. A hit would be considered successful if the staff at the branch let the social engineer into the premises without verifying from the ICT department whether the social engineer was who he/she claimed to be. The successful hits in each of the branches are illustrated below.

	Successful hits
Branch 1	1
Branch 2	1
Branch 3	0

Table 10: Pretexting and Role Playing

From the analysis of the data, it was established that the Branch 1 had one hit same as Branch 2. Access to Branch 3 would be considered unsuccessful as the staff took the initiative to place a call to the IT department for verification. Branch 1 and 2 can be considered as a risk area as the staff did not take any initiative to verify the identity and mission of the social engineer from the relevant parties in this case the IT department.

The success of the exercise on Branch 1 and 2 can be attributed to the high human traffic as compared to Branch 3 so it was somewhat easier for the social engineer to convince the 'overwhelmed staff'. To curb such incidences in future the organization needs to educate the entire

organization and not just IT on social engineering and also establish clear communications within the organization.

4.8 Correlation Analysis

The study sought to establish the relationship between the social engineering techniques and threat/risk factor in the organization. Pearson Correlation analysis was used to achieve this end at 95% confidence level ($\alpha = 0.05$).

Social engineering techniques	**Threat/risk factor**	
Shoulder Surfing	Pearson Correlation	0.686**
	Sig. (2-tailed)	.002
Dumpster diving	Pearson Correlation	0.690*
	Sig. (2-tailed)	.023
Pretexting /role playing	Pearson Correlation	0.719**
	Sig. (2-tailed)	.005
Surfing organizational websites	Pearson Correlation	0.428**
	Sig. (2-tailed)	.001

Table 11: Correlation

Correlation is significant at the 0.05 level (2-tailed).*

Correlation is significant at the 0.01 level (2-tailed). **

The table above shows that there were significant correlation coefficients established between the social engineering techniques and threat/risk factor.

For the absolute value of *r* Evans (Evans, 1996)suggests:

- .00-.19 “very weak”
- .20-.39 “weak”
- .40-.59 “moderate”
- .60-.79 “strong”
- .80-1.0 “very strong”

Very good and positive linear relationships were established among the independent and dependent variables: shoulder surfing (R = 0.686, p =.002); dumpster diving (R = 0.690, p = .023); Pretexting/role playing (R = 0.719, p = .005); and surfing organizational websites (R = 0.428, p = .001). This depicts that the social engineering techniques positively enhance the threat/risk factor.

4.9 Regression Analysis

The study sought to establish how various social engineering techniques employed by hackers to gain access to organization's data or information enhances the threat/risk level using multiple linear regression analysis. The techniques were: shoulder surfing, dumpster diving, Pretexting/role playing, and surfing organizational websites. The regression model was:

$Y= \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \beta_5 X_5 + \beta_6 X_6 + \varepsilon$

Whereby Y is threat/risk factor , β_0 is regression constant, $\beta_1 - \beta_6$ regression coefficients where X_1 is shoulder surfing, X_2 is dumpster diving, X_3 is pretexting/role playing, X_4 is surfing organizational websites and ε, the model's error term. The table below shows that there is a good linear association between the dependent and independent variables used in the study. This is shown by a correlation (R) coefficient of 0.887. The determination coefficient as measured by the adjusted R-square presents a strong relationship between dependent and independent variables given a value of 0.764. This depicts that the model accounts for 76.4% of the variations in threat/risk factor while 33.6% remains unexplained by the regression model.

Durbin Watson test was used as one of the preliminary test for regression which to test whether there is any autocorrelation within the model's residuals. Given that the Durbin Watson value was close to 2 (2.104), there was no autocorrelation in the model's residuals.

Model's Goodness of Fit Statistics

R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
.887[a]	.787	.764	.757	2.104

Table 12: Model's Goodness of Fit Statistics

a. Predictors: (Constant), shoulder surfing, dumpster diving, pretexting/role playing, and surfing organizational websites.

b. Dependent Variable: High security risk factor

4.10 Analysis of Variance (ANOVA)

The ANOVA statistics presented in the table below was used to present the regression model significance. An F-significance value of $p < 0.001$ was established showing that there is a probability of less than 0.1% of the regression model presenting false information. Thus, the model is very significant.

	Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Regression	120.450	5	20.075	35.037	.000[b]
Residual	32.659	32	.573		
Total	153.109	37			

Table 13: Analysis of Variance (ANOVA)

a. Predictors: (Constant), shoulder surfing, dumpster diving, pretexting/role playing, and surfing organizational websites.

b. Dependent Variable: High security risk factor

4.11 Regression Coefficients

From the findings in the table below, the multiple linear regression equation becomes:

$Y= 2.653 + 0.316X_1 + 0.003X_2 + 1.403X_3 + 0.570X_4$

From the model, when other factors (shoulder surfing, dumpster diving, Pretexting/role playing and surfing organizational websites) are at zero, the high threat/risk factor is noted to be 2.653. Holding other factors (shoulder surfing, dumpster diving, Pretexting/role playing and surfing organizational websites) constant, a unit increase in shoulder surfing instances would lead to a 0.316 ($p = .002$) increase in threat/security risk factor.

Holding all other independent variables constant, a unit increase in dumpster diving would lead to a 0.003 ($p = .023$) increase in high security risk factor. Holding shoulder surfing, Dumpster diving and surfing organizational websites constant, a unit increase in pretexting/ role playing would lead to a 1.403 ($p <.001$) increase in threat/security risk factor.

Also noted is that, holding shoulder surfing, dumpster diving and Pretexting/ role playing, a unit increase in the independent variable surfing organizational websites would lead to a 0.552 ($p <.001$) increase in threat/security risk factor. This shows that among the social engineering techniques, Pretexting/role playing followed by surfing organizational websites, shoulder surfing and dumpster diving would have the most positive influence on high security risk factor.

Social engineering techniques	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	2.653	.861		10.055	. 983
Shoulder surfing	.316	.097	.270	3.268	.002
Dumpster diving	.003	.137	.002	.022	.023
Pretexting/role playing	1.403	.141	.998	9.925	.000
Surfing organizational websites	.462	.204	.328	2.260	.028

Table 14: Regression Coefficients

a. Dependent Variable: high security risk factor

4.12 A Chi-square Analysis

This is to establish the risk analysis of the social engineering practices in relation to high security risk factor

4.12.1 The relationship between shoulder surfing and threat/risk factor

The study investigated the threat/risk extent of shoulder surfing as a social engineering technique. The findings are as shown in the table below. The results as indicated depict a chi-squared test statistic of 19.19 with associated Chi-Square, likelihood ratio and linear-by-linear association p, which is > 0.05. Therefore, there is statistically significant relationship between shoulder surfing and threat/risk factor.

	Value	Df	Asymp. Sig. (2-sided)
Pearson Chi-Square	19.195[a]	3	.10
Likelihood Ratio	18.388	3	.0520
Linear-by-Linear Association	7.573	1	.083
N of Valid Cases	150		

Table 15: Test of significant risk analysis between shoulder surfing and threat/risk factor

4.12.2 Relationship between dumpster diving and threat/risk factor

The study further sought to find out the relationship between dumpster diving and threat/risk factor and the findings are as stipulated in the table below. The results depict a chi-squared test statistic result of 11.65 with associated Chi-Square, likelihood ratio and linear-by-linear association p,

which is > 0.05. There is statistically high risk of dumpster diving as a social engineering technique but the risk ratio is lower than that of shoulder surfing.

	Value	**Df**	**Asymp. Sig. (2-sided)**
Pearson Chi-Square	11.654[a]	9	.063
Likelihood Ratio	13.020	9	.082
Linear-by-Linear Association	3.200	1	.094
N of Valid Cases	150		

Table 16: Test of significant relationship between dumpster diving and threat/risk factor

4.12.3 Relationship between Pretexting/role playing and threat/risk factor.

The study further sought to find out the relationship between Pretexting/dumpster diving and threat/risk factor and the findings are as stipulated in the table below. The results depict a chi-squared test statistic result of 6.509[a] with associated Chi-Square, likelihood ratio and linear-by-linear association p, which is > 0.05. There is statistically high risk in Pretexting/role playing as a social engineering technique but the risk ratio is lower than that of shoulder surfing or dumpster diving.

	Value	**Df**	**Asymp. Sig. (2-sided)**
Pearson Chi-Square	6.509[a]	2	.009
Likelihood Ratio	10.326	2	.006
Linear-by-Linear Association	4.738	1	.000
N of Valid Cases	150		

Table 17: Test of significant relationship between Pretexting/role playing and threat/risk factor.

4.12.4 Relationship between surfing organizational websites and threat/ risk factor

The study further sought to find out the relationship between surfing organizational websites and treat/risk factor and the findings are as stipulated in the table below. The results depict a chi-squared test statistic result of 4.382[a] with associated Chi-Square, likelihood ratio and linear-by-linear association p, which is > 0.05. There is statistically high risk in Pretexting/role playing as a social engineering technique but the risk ratio is lower than that of shoulder surfing, dumpster diving, or Pretexting/role playing.

	Value	**Df**	**Asymp. Sig. (2-sided)**
Pearson Chi-Square	4.382[a]	2	0.012
Likelihood Ratio	4.390	2	0.011
Linear-by-Linear Association	2.593	1	0.007
N of Valid Cases	150		

Table 18: Test of significant relationship between surfing organizational websites and threat/security risk factor

CHAPTER 5-CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter is a synthesis of the entire study, and contains summary of research findings, exposition of the findings, commensurate with the objectives, conclusions and recommendations based thereon.

5.2 Achievements of the study

Various social engineering techniques were explored during this study and observation was mostly used as the personnel in the organization went about their day to day activities. What made the exercise a success was the fact that management granted the authority for the exercise to be carried out within the organization premises and also the personnel had no prior knowledge of the exercise to ensure authenticity of the data being collected.

Motives and factors that influence the success of a social engineering attack were highlighted in detail. The motives include but are not limited to Financial gain, Personal interest, External pressures, Intellectual challenge, Damage containment, Personal grievance and Politics.

The factors highlighted were further categorized into Personality traits, Human factors and Organizational factors. The determination of risk areas was done by use of questionnaires and observation.

The questionnaire was used to establish risk levels the organization is exposed to by assessing the stakeholders' awareness levels in regards to information security. The findings indicated that the risk level was **Moderate** meaning that the users are aware of threats and know they should follow good security principles and controls but need training on organizational security standards and policies. They also may not know how to identify or report a security event.

Observation was carried out in the following social engineering techniques.

Shoulder Surfing- the departments observed were Claims, Human Resources, Underwriting and Finance. From the results obtained, Finance department was ranked as the one that posed the highest risk due to the fact that they had systems which held information considered as very sensitive e.g. online banking portals and access to these by a social engineer would cause the organization severe damage.

Dumpster Diving- Departments observed were Human Resources, Finance and Underwriting. Again Finance Department was considered the one that posed the highest risk considering some of the data retrieved e.g. blank petty cash vouchers would cause considerable damage if it fell in the wrong hands.

Surfing Organizational Websites and Social pages- Contacts and names for various branch and departmental heads were obtained during this exercise. No ranking at this stage as it was

considered an information gathering exercise for the Social Engineer for him/her to successfully carry out an attack such as pretexting/role playing.

Pretexting/Role Playing- Two out of the three branches proved to be vulnerable in terms of access by outside parties thus posing as possible security risks.

5.3 Limitations

1. It was not possible to carry out a phishing attack simulation due to concerns raised by the ICT Management owing to recent attempts on the organization's IP Telephone servers.
2. Time was limited to facilitate for further tests to be carried out after awareness levels had been introduced among the stakeholders e.g. through Security Awareness Workshops so as to determine whether there would be any improvement noted against the results obtained from this study.
3. It was not possible to compare security practices among the different companies in the insurance sector in Kenya due to restrictions such as Non-Disclosure Agreements signed by staff due to industry competition.

5.4 Conclusion

The study made use of questionnaires and observation of various social engineering techniques and from these it is clear that the awareness levels displayed in the questionnaires are reflected in what was observed in the stakeholders as they went about their duties. Through observation the study explored various social engineering techniques and from these it can be concluded that the organization faces a threat/risk if any of the techniques were to be used by a social engineer in the case an actual attack occurred. The information security awareness levels displayed by the stakeholders from the results of the questionnaires also indicate that the organization faces a potential threat/risk in regards to social engineering.

The output presented by these techniques indicate that social engineering being a 'non-technical' way of infiltration should be taken seriously as any other technical threat. It is therefore important for continuous research to be carried out in this field as the field of social engineering is dynamically changing with the advancement of technology.

5.5 Recommendations

User Awareness and Education

Stakeholder awareness and acceptance of safeguard measures should become the first line of defense in the battle against the attackers. Humans being the weakest link in any security setup, need to be educated about the dangers of social engineering and how it can manifest itself in the organization

Trainings should be a frequent occurrence and can include; employee indoctrinations, security awareness briefings, and periodic newsletters. Taking a more active stance, practical testing and demonstration of stakeholders' vulnerability can have value, if conducted in an ethically-sensitive manner. Many stakeholders would actually be appreciative of being alerted in this way rather than falling victim to a genuine incident.

The stakeholders need to ask for some form of authentication or identification when approached by a 'stranger' soliciting for information. To ensure the training sessions are effective, policies, procedures and standards must be taught and reinforced to everyone in the organization.

Security Policies

Establishing and enforcing a clear anti-social engineering policy can be very effective. These are basically standards and guidelines that entail the rules that work against social engineering and a user is required to follow. The security policy should be well-documented with sets of standards that form a strong foundation of a good security strategy. It should clearly document in simple terms, its scope and contents in each area that it applies to. Every new user should be oriented on the security policies that they are expected to follow. There is need to carry out a thorough risk assessment before creation of the policy so as to identify the areas that need to be covered.

Security Audits

Developing and implementing security policies is not enough. There is need to ensure that everyone conforms to the policy. For this reason, there is need to have audits on the implementation of the policies. These audits should be done across the board in an organization. Periodic security vulnerability assessments and penetration tests should be conducted in the organization so as to keep the security policy up to date on emerging social engineering threats.

Physical Access Authentication

Physical security will help minimize the chance of a social engineer from gaining access to the organizations' premises. All authorized personnel are needed to have a form of identification card that should be produced at the entrance of the premises or particular areas within the organization. Where there is doubt, confirmation needs to be acquired through the relevant authorities. Visitors should be escorted to where they need to go and be required to wear a badge indicating the department or level in the organization that they intend to visit.

Incident Documentation and Reporting

Comprehensive security incident reporting helps to provide the organization with an accurate picture of events affecting the organization and enables it to prepare and respond appropriately. It is the responsibility of all stakeholders of the organization to promptly report all security incidents occurring within the organization environment, actual or suspected (including matters which may

have already been reported to police), to the organization's security team. Reporting incidents of compromise can greatly reduce the impact of an active attack if it is still running.

Documenting these incidents is crucial as it will serve as a reference point in case a similar attack occurs, the security team can go through the measures taken then and how effective they were and form a basis whether an update is needed in light of the new attack.

Documentation and reporting also helps in identifying attack patterns that are employed against the organization.

Caution among 'unfamiliar' persons

Users must be cautious of unfamiliar individuals and not give out information unless there is a confirmation of their identity. The Human Resource department should timely communicate deployment of new staff to the various departments or branches so as to prevent cases of impersonation by unscrupulous people.

Employee Background Checks

Not all new employees have the goals of the organization at heart. Some people join an organization so that they can gather and disclose as much information as possible on behalf of a competitor. It is important for employers to carry out thorough background research on new employees or would be employees for consistency checks.

Waste Disposal

Waste office paper should be destroyed via a paper shredder before being disposed-off in the trash can or put in an incinerator if a shredder is not available. The waste should be unreadable to anyone. Every work area will require to have a shredder. This will eliminate the possibility of confidential information to be collected from trash cans. Any digital information should be disposed of in ways stipulated in the policy.

Appreciating the value of information

Stakeholders also need to be more aware of their own data and why it is sensitive. For example, there is a significant potential for data-scraping from social networking sites such as Facebook and Twitter, with attackers lifting information that users themselves have placed there with little regard for who could see it and how it could be misused. User pages on the aforementioned sites are often littered with details such as dates of birth, addresses, personal interests, family background and employment details, with many users exercising no caution in how widely they share it. This can work against the individual in both personal and workplace scenarios, with the consequence that they could end up being convinced that someone knows enough about them to be trusted purely by virtue of the details that they themselves have made publically available online**.** From a similar perspective, organizations need to consider what they do with information – including what they dispose of and what they put on public display. To what extent are they rendering their own staff

more susceptible to social engineering by making details available that someone else could use in an attempt to deceive them? For example, listing things like staff names and roles on a website gives a would-be attacker an immediate insight into who can be contacted for what, and whose name could be dropped in to add legitimacy. (ENISA, 2008)

5.6 Enterprise Risk Management

5.6.1 COSO ERM in Social Engineering

The following is a customization of the COSO ERM with a focus on social engineering.

5.6.2 Control Environment

The rapid evolvement in ICT continues to play a major role in transforming how organizations operate globally. It has opened up an avenue in which organizations can share information with various external parties such as service providers, regulators or even other organizations within their industry with a lot of ease. The digital reach is not limited but geographic boundaries which leads to a heavy dependence on complex infrastructure which the organizations have little or no control over. With this ease in communication, there emerges problems on how they can best secure this information that is being shared. Malicious parties will always look for means to try and exploit any vulnerabilities in information systems so as to obtain such information. What they do with such information is open to infinite possibilities that the organizations involved cannot risk fall victim.

As much as organizations may take all the necessary precautions to safeguard their information both internally and externally, social engineers on the other hand can afford some flexibility in their operations without really having to worry about any set regulations or ethical issues. Social engineers will openly share information among themselves in an anonymous fashion which makes their attacks which can happen from anywhere in the globe very successful and nearly untraceable at the same time.

Putting into consideration how organizations' objectives, methodology and technology will continue to evolve over the years, it is safe to accept that protecting all information is not possible. With each evolution a vulnerability is created and it is not possible to manage evolution with foolproof certainty that such vulnerabilities will not be exploited. With such, social engineers are also evolving and are developing new ways with which to carry out their attacks. Social engineering as a threat cannot be fully eliminated but it can be managed to levels that are acceptable within an organization's risk appetite.

By classifying data according to its importance to the organization and risk that it may bring about as a result of compromise, the stakeholders must invest in controls and practices that will ensure

vigilance, security and resilience. This will bring about some confidence on the security of their information and help them remain focused on their quest to achieving their strategic objectives. When organizations view their cyber profile through the components of Internal Control, it will go a long way in helping them manage the social engineering threat/risk. For example:

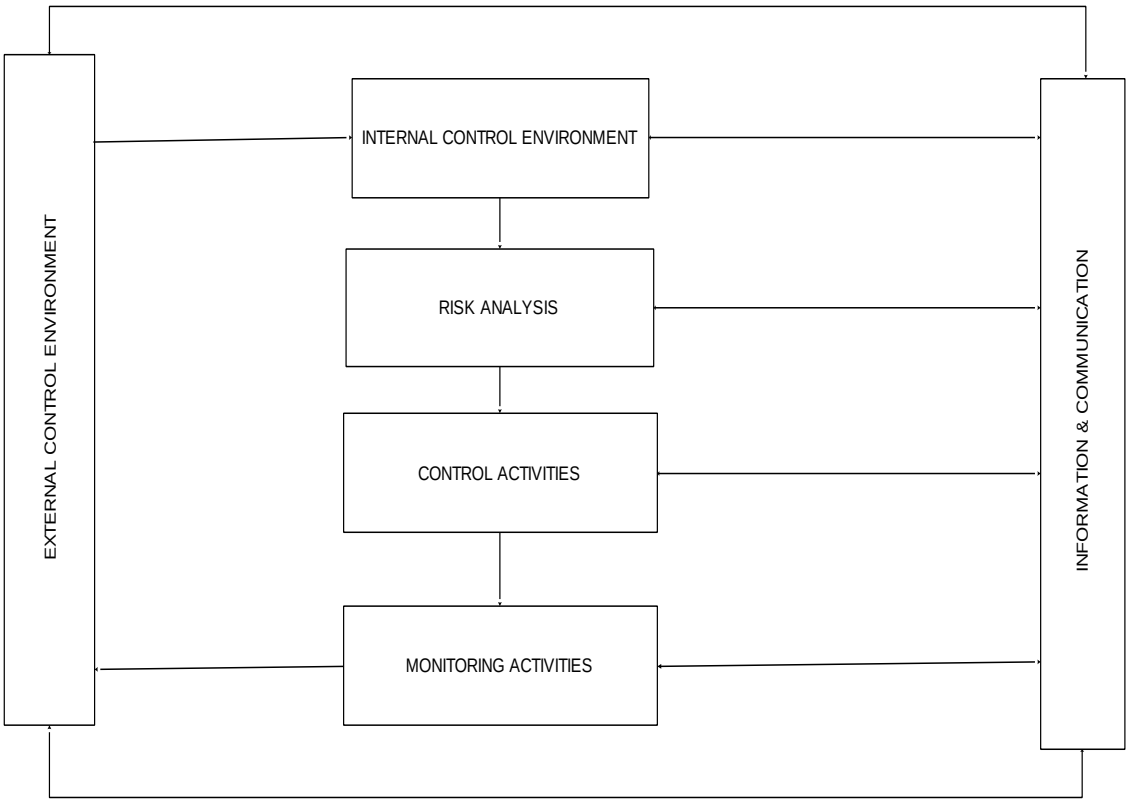


Figure 4: Customized ERM Framework

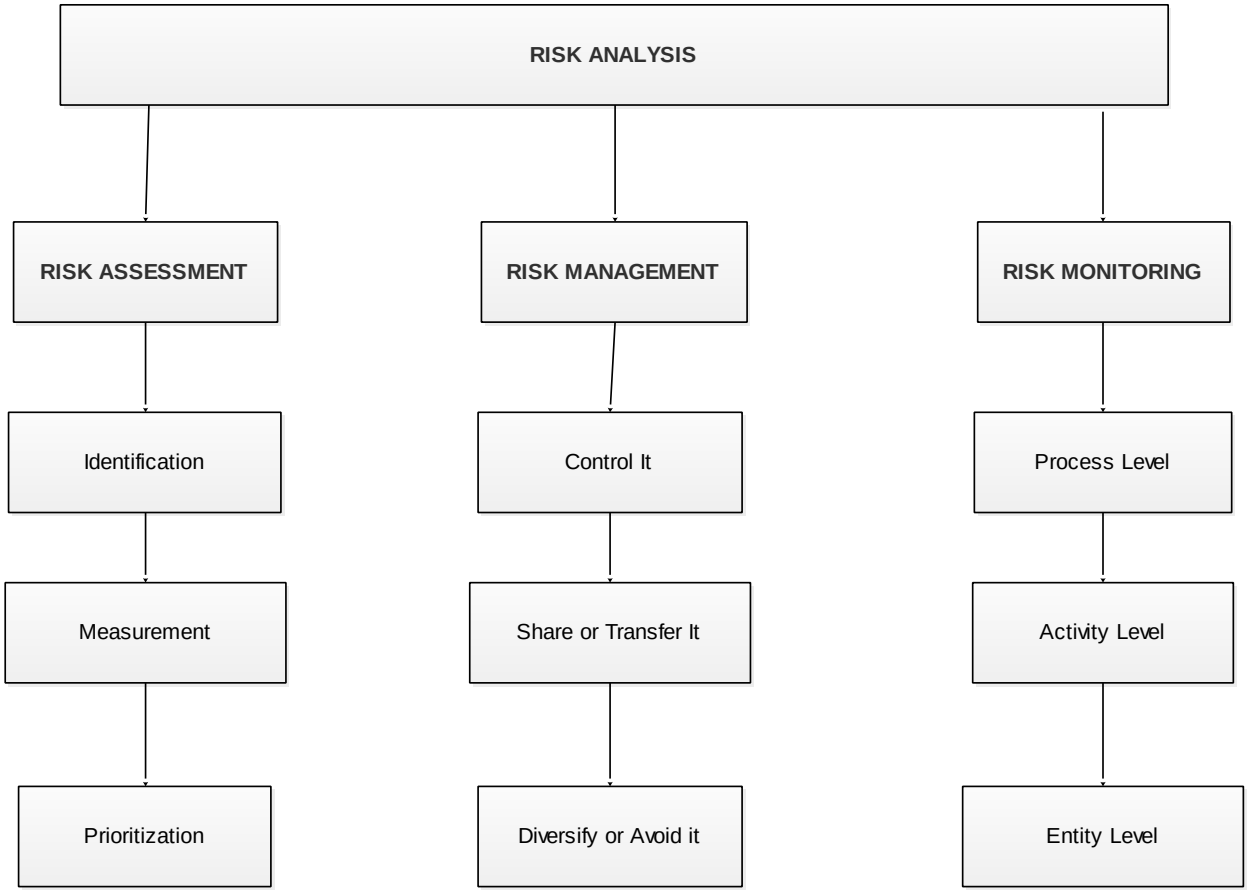
Control Environment – this ensures that the Decision Makers have an understanding of the cyber risk profile of the organization and are informed of how the organization is managing the evolving social engineering threats that it may face. This can be further categorized into:

Internal Control Environment. This sets the tone of the organization, influencing risk appetite, attitudes towards risk management and ethical values. The company's tone is set by the Decision Makers which in most organizations is the board of directors and senior management. A board that lacks the technical knowledge, experience, diversity and voices with authority amongst them may not succeed in setting the right tone.

External Control Environment. One criticism of the COSO ERM model has been that it starts at the wrong place. It should begin with the external and not the internal environment. By ignoring

the external environment, the impact of elements such as competitors, regulators and other external stakeholders is not reflected sufficiently on the organizations risk appetite in regards to social engineering risks/threats. It is with this mindset that this ERM model encompasses the external environment as threats are not confined to only the internal environment.

Risk Analysis –This ensures that the organizations' stakeholders have carried out an evaluation on the operations, financial, performance and compliance objectives. The information obtained thereafter will help in understanding how a social engineering threat/ risk may impact the said objectives. The human aspect (Recruitment, people skills, health) should also be considered during risk this stage.



(Institute of Internal Auditors, 1998)

Figure 5: Risk Analysis

Control Activities-This helps to ensure that the organization has developed control activities over technology which will aid in managing social engineering risks/threats within its acceptable risk appetite levels. This stage also ensures that the control activities are deployed through the set policies and procedures.

Information and Communication **–** Identification of information requirements will help in managing internal and external control over social engineering threats/risks. Internal and external

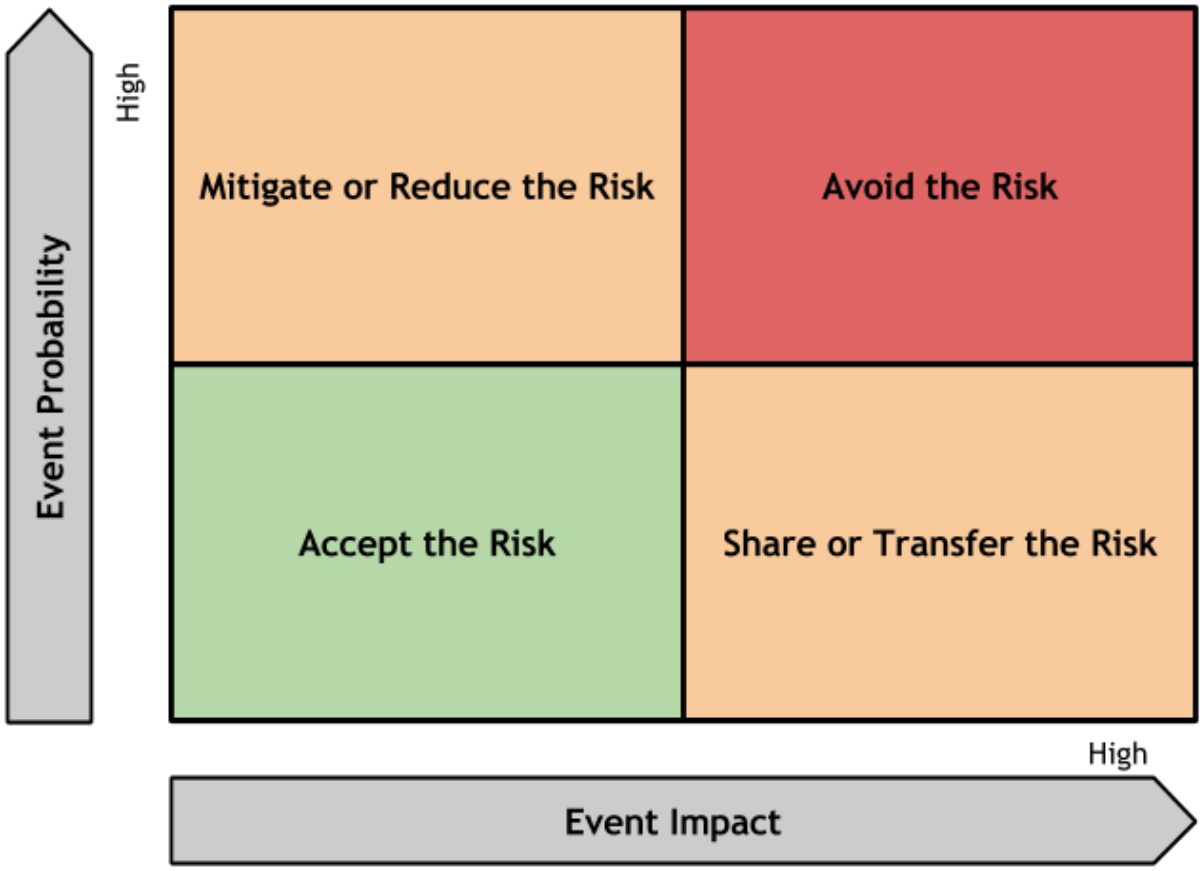
communication channels are also identified at this stage. How the organization responds to manage and communicate a social engineering incident is also addressed at this stage. Proper dissemination of information ensures that a potential or existing threat regardless of its size is known by the relevant stakeholders in the organization in a timely manner. This should happen at every component of the framework and can take any approach in the organization for example top-down or bottom-up approach. This is to ensure that a potential threat no matter how small is known to the stakeholders in the organization.

Monitoring Activities **–**This is how the organization performs its evaluations to check on the effectiveness of both internal and external controls that address social engineering risks/threats. Where shortfalls are identified, they should be timely communicated and corrective action prioritized. Monitoring of an organizations risk profile should be a continuous activity and the stakeholders need to update themselves with the emerging trends of threats in relation to social engineering.

5.6.3 A COSO-focused Social Engineering Threat/Risk Assessment

Every organization faces a variety of social engineering threats/risks from external and internal sources. Social engineering threats/risks should be evaluated against the probability of an incidence occurring thereby negatively affecting the achievements of the organization's objectives.

An organization's social engineering threat/risk assessment should begin by identifying the information and information systems that are of value. The assessment should also identify the personnel and departments that have been entrusted to both the information and information systems. This should be measured against the potential impact to the event probability. Below is an event probability and event impact matrix.



(OWASP, 2013)

Figure 6: Event Probability & Event Impact matrix

As much as the results of the risk assessment will justify the allocation of resources against control activities which will be used to prevent, detect and manage the social engineering threats/risks, resources should also be allocated to the risk assessment process itself. As the risk assessment informs the Decision Makers' and Senior Managements' decisions about measures put in place against information and information systems, it is important that they communicate to the relevant stakeholders on these measures and what is to be safeguarded in alignment to the organization's strategic objectives. This will require a collaboration between business and IT stakeholders.

For the assessment process to be effective the involved parties must have a clear understanding of the organization's social engineering threat/risk profile. This will involve understanding the information systems that potential perpetrators might find valuable and also understand the methodologies that may be used to carry out the attacks.

The risk assessment process should be continuous and updated regularly as the threat landscape keeps evolving with the advancement in technology. The information acquired therein should be help the Decision Makers and Senior Management make informed decisions on how best to counter the social engineering threats/risks.

Identifying and Implementing Control Activities that Address Social Engineering Threats/Risks

Control activities are carried out by all the stakeholders within the organization so as to ensure the guidelines and directives laid down by the board and senior management are followed in the quest to mitigate risks posed by social engineering risks/threats as they try to achieve the organization's objectives. These activities should be clearly spelt out in the policies so as to ensure consistency in their execution throughout the organization.

Social engineering threats/risks are unavoidable, but with careful design and implementation of controls such risks can be managed to acceptable levels. Through the risk assessment process where the likely attack methods and routes are considered, an organization will be in a better position to minimize the negative impact that an actual social engineering attack may have on its set objectives.

An organization can have many entry points that can serve to expose it to the threat of a social engineering attack. As such preventive and detective measures should be deployed both internally and externally. Properly designed measures may help prevent intruders from gaining access into the organization's perimeter thus keeping the internal environment relatively safe. Additional preventive measures should be deployed internally to further slowdown intruders who may have succeeded in gaining entry into the organization's infrastructure. This will help the organization with timely detection of breaches and corrective measures can be taken as well as assessment of potential damages can be carried out as early as possible. The root cause of the breach should be investigated after the corrective measures have been put in place to detect and prevent a similar occurrence in future by improving the current controls in place.

Informs and Communicates

It ensures information and communication generated is relevant and has the quality to manage social engineering risks and controls. This component is composed of three principles that aid organizations to focus their efforts on:

Identifying quality and relevant information

Definition of how information should be disseminated internally and

Definition of how the organization is supposed to communicate with external parties.

Identifies Information Requirements

The information requirements are dictated by the controls put in place within the organization. The information can be in form of reports or overview diagrams that demonstrate the organization's business structure at a higher level view.

Processes Relevant Data into Information

Security systems can generate a huge amount of logs on a daily basis originating from the various events in the information systems such as but not limited to successful and successful logins into the systems. For vigilance with respect to the social engineering risks/threats, it is prudent for the raw data collected to be transformed to meaningful information with integrity that can be acted upon.

Social engineering exploits cannot be identified through a single event but a series of events through which a pattern can be identified which can lead to action against potential exploits. If the raw data is not transformed to meaningful information, an organization cannot timely act in case a breach has occurred as it will be next to impossible to trace the possible origin or point of exposure. This control is fully dependent on the timely delivery of relevant and quality information that has integrity.

Captures Internal and External Sources of Data

As much as the primary source for information for social engineering threat/risk analysis and controls is generated internally, it is very crucial for organizations to consider external data. The following are sources of external data. The list is not exhaustive but is relevant for most organizations.

Industry Focused External Data: Every organization's operations are based within an industry profile that has similar patterns when it comes to a cyber-security perspective. Such organizations within an industry tend to have similar information systems both in value and operation technologies. For example, insurance companies share the claim history of their clients which enables a company to determine the risk worthiness of a client. It also aids in giving clients who have not filed a claim in a particular period of time a discount commonly referred to as Non Claim Discount. This similarity often goes a long way in dictating the behavior of attackers and the attack methods that they may use. As much as externally sharing information should be done with a lot of care, there can be numerous benefits achieved especially when discussing emerging social engineering trends between industry groups to further reduce the likelihood of an attack.

Government Agency External Data: Government agencies such as the Insurance Regulatory Authority (IRA) and Kenya Revenue Authority (KRA) advocate for improving processes and controls that will ensure the organizations are defended against the ever evolving threat cyber-attacks.

Outsourced Service Provider External Data: In the world we live in today it is inevitable that organizations will outsource certain functions and processes from other external parties for various reasons. As such it is prudent for these organizations to share their cyber profiles with a complete view of the controls put in place. Transparency and collaboration between the organizations can

prove to be very vital if either organization experiences a social engineering incident which may end up having a negative impact on either organization's operations.

Maintains Quality throughout Processing

For the quality of information in the organization to be maintained there should be clear map of who is responsible and accountable and this should be supported by sticking to the expectations of data governance that help in protecting information against unauthorized access or change. Data governance is the determinant of an organization's ability to generate and use quality information that is relevant to support the functioning of the external and internal control. With an effective data program established and the organization practices discipline to maintain the program then information quality attributes can be realized. Information quality goes a long way in improving the organization's overall system of internal and external control further helping in improving controls against social engineering risks/threats. Attributes of Quality Information are but not limited to Accessible, Correct, Current, Protected, Sufficient, Timely, Valid, Verifiable and also Retained.

To Communicate Internal and External Control Information

To All Stakeholders

Security, vigilance and resilience is an organizational responsibility as a whole and should not solely be an individual responsibility. As much as specific individuals may be explicitly empowered to manage the risks and controls, each stakeholder within the organization should play a role in securing the information and information systems within and outside the organization. A cyber risks and controls program should be established throughout the organization as such will help strengthen what is often considered the weakest link in information security, that is the human element. The communications should be on a regular basis to enhance the awareness of social engineering and reduce the probability of success in the case a social engineering attack were to occur.

To those Responsible for Managing and Monitoring Social Engineering Threats/Risks and Controls

Those responsible for managing and monitoring social engineering risks and controls are mostly comprised of the IT department within the organization and external parties such as system auditors. It is crucial for them to document all the controls that have been put in place as without proper documentation the ability of the organization to effectively manage any social engineering risk/threat is highly reduced.

To the Decision Makers

This group is comprised of the board of directors and senior management. They should be able to demonstrate their ability to understand and stay abreast of emerging cyber trends that could

negatively and positively impact the organization's quest to achieve its strategic objectives. There should be clear and effective communication channels between the Decision Makers, Technical Experts and the Users in general. The Technical experts are responsible for interpreting complex IT terminologies in ways that make sense to the decision makers. This is critical as it will help them better exercise internal and external control oversight responsibilities.

Regularly scheduled communications at the decision maker level should include updates on social engineering trends delivered in a timely manner when major social engineering incidences are identified.

With External Entities

Enforcing policies and standards to manage and control external communications is very important. It is very important to manage risk when communicating externally so as to reduce the potential for negative impacts to the organization.

Control Environment and Monitoring Activities

These activities are essential for an organization to properly manage its social engineering threat/risk exposures. Control environment provides the basis for carrying out internal and external control across the organization. The decision makers set the tone in the emphasis of the importance of internal and external control and standards of conduct that are expected to be maintained. They should define security, vigilance and resilience as a priority and clearly and timely communicated within the organization. This will ensure that sufficient resources are deployed in protecting the organization's information and information systems and also facilitate for timely response to social engineering incidences in good time. With the collaboration of business and technical experts, complex IT topics related to social engineering and cyber security in general must be translated against the organization's strategic objectives and priorities.

The following are keys to Effective Control Environment and Monitoring of Social Engineering Threats/Risks:

1. Clear tone and communication channels from the top regarding why it is important to protect information and information systems.
2. Continuous evaluations to assess the structure and effectiveness of controls that have been put in place with an aim to reduce potential social engineering exposures.
3. Collaboration between qualified information security experts and business experts so as not to stay focused on the organization's strategic objectives
4. Continuous monitoring of social engineering risks and controls that may originate from both internal and external entities
5. Clear and timely communication of cyber security shortcoming and ways to remedy them in the shortest time possible.

6. Enforcing a sense of responsibility and accountability to those entrusted with the organization's information and information systems.

Conclusion

When an organization reviews their cyber risk profile through this customized COSO lens, it may reconsider how it can influence change that will influence change and in turn improve their controls when it comes to mitigating the threats/risks posed by social engineering to the organization. Security, vigilance and resilience will and should be a priority for the organization. Social engineering threats/risks should be dealt with in a proactive not reactive manner as doing so will greatly reduce the severity of potential attacks. As technology evolves, so do the social engineers themselves and this will make it extremely difficult to manage. Recognizing social engineering as a serious cyber security threat should influence the organization towards investing in controls and activities to help reduce the negative impact of an attack if it were to occur. This will not only keep the organization's information and information systems secure but it will also help it keep its focus towards the actualization of its strategic objectives.

REFERENCES

Allen, M., 2006. *Social Engineering: A Means To Violate a Computer System.*. [Online]
Available at: http://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529
[Accessed 9 April 2014].

Alseadoon, I., Chan, T., Foo, E. & Nieto, J. G., 2012. *Who is more susceptible to phishing emails?: A Saudi Arabian study.* Australia, s.n.

Anon., 2014. *Phone cash scams that leave clients penniless.* [Online]
Available at: http://nairobinews.co.ke/phone-scam/
[Accessed 15 December 2014].

Bailey, K. D., 1987. *Methods of Social Research.* 3 ed. Michigan: Free Press.

Bishop, M., 2004. *Introduction to Computer Security.* 1 ed. s.l.:Addison-Wesley Professional. .

Bitpipe, n.d. *Bitpipe Research Guide: Security Overview.* [Online]
Available at: http://www.bitpipe.com/security/security_overview.jsp
[Accessed 8 December 2014].

Bond, T., n.d. *SANS.EDU.* [Online]
Available at: http://www.sans.edu/student-files/awareness/employee-security-awareness-survey.pdf
[Accessed 27 January 2015].

Bulgurcu, B., Cavusoglu, H. & Benbasat, I., 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, 3 September, pp. 523-548.

Business Dictionary, n.d. *BusinessDictionary.com.* [Online]
Available at: http://www.businessdictionary.com/definition/motive.html#ixzz3ThdJ39lK
[Accessed 7 March 2015].

Business Dictionary, n.d. *Hypothesis.* [Online]
Available at: http://www.businessdictionary.com/definition/hypothesis.html#ixzz3Q0aIOrQO
[Accessed 27 January 2015].

Business Dictionary, n.d. *Research Design.* [Online]
Available at: http://www.businessdictionary.com/definition/research-design.html
[Accessed 25 2 2015].

Business Dictionary, n.d. *Target Population.* [Online]
Available at: http://www.businessdictionary.com/definition/target-population.html
[Accessed 25 2 2015].

Cherry, K., n.d. *About.com Psychology.* [Online]
Available at: http://psychology.about.com/od/hindex/g/hypothesis.htm
[Accessed 15 July 2014].

Cooper, , D. R. & Schindler, P. S., 2008. *Business Research Methods.* 10 ed. s.l.:McGraw-Hill.

COSO, n.d. *Guidance on Enterprise Risk Management.* [Online]
Available at: http://www.coso.org/-erm.htm
[Accessed 1 4 2016].

Creative Research Systems, 2015. *Creative Resaerch Systems.* [Online]
Available at: http://www.surveysystem.com/sscalc.htm#one
[Accessed 10 June 2015].

Deloitte, 2015. *Deloitte.* [Online]
Available at: http://www2.deloitte.com/be/en/pages/risk/articles/insurance.html
[Accessed 22 5 2015].

Dhamija, R., Tygar, J. D. & Hearst, M., 2006. "Why Phishing Works". *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* Volume CHI 06, pp. 581-590.

Digman, J. M., 1990. "Personality Structure: Emergence of the Five-Factor Model.". *Annual Review of Psychology,* Volume 41, pp. 417-441.

Downs, J. S., Holbrook, M. B. & Cranor, L. F., 2007. *Behavioral Response to Phishing Risk.* Pittsburgh, PA,, ACM.

ENISA, 2008. *Social Engineering: Exploiting the weakest links.*. [Online]
Available at: http://www.enisa.europa.eu/publications/archive/social-engineering
[Accessed 4 6 2014].

Erkkila, J., 2011. *"Why We Fall for Phishing" Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* Vancouver, BC, Canada,, CHI 2011.

Evans, J. D., 1996. *Straightforward Statistics for the Behavioral Sciences.* Pacific Grove, California: Brooks/Cole Publishing.

Galligan, E. M. & Rau, K., 2015. *COSO in the Cyber Age.* [Online]
Available at: www.coso.org
[Accessed 25 March 2015].

Galligan, M. E. & Rau, K., 2015. *COSO in the Cyber Age.* [Online]
Available at: http://www2.deloitte.com/us/en/pages/risk/articles/coso-in-the-cyber-age-research-report.html
[Accessed 25 3 2015].

Hadnagy, C., 2011. *Social Engineering: The Art of Human Hacking*.. Indianapolis: Wiley Publishing Inc..

Halevi, T., Lewis, J. & Memon, . N., 2013. *Phishing, Personality Traits and Facebook*.. [Online]
Available at: http://arxiv.org/abs/1301.7643
[Accessed 15 June 2015].

Hitchcock, D., 2005. *Evolution of Information Security Technologies,* s.l.: s.n.

IBM Global Technology Services, 2007. *The Evolving Threat: Combat training for the new era of malicious code.*. [Online]
Available at: https://www-304.ibm.com/easyaccess/fileserve?contentid=131594
[Accessed 8 December 2014].

Institute of Internal Auditors, 1998. *Applying COSOs Enterprise Risk Management-Integrated Framework,* s.l.: s.n.

ISO, n.d. *ISO 31000 - Risk management.* [Online]
Available at: http://www.iso.org/iso/home/standards/iso31000.htm
[Accessed 1 4 2016].

Jakobsson, M., 2007. *"The Human Factor in Phishing." Privacy & Security of Consumer Information'07..* [Online]
Available at: http://markus-jakobsson.com/papers/jakobsson-psci07.pdf

Kahneman, D. & Tversky, A., 1979. *"Prospect Theory: An Analysis of Decision under Risk.",* s.l.: s.n.

Kantarcioglu, M., n.d. *Overview of Information Security*, s.l.: UTDALLASS: Erik Jonsson School of Engineering & Computer Science.

Kigen, P. et al., 2014. *Kenya Cyber Security Report 2014.* [Online]
Available at: http://www.serianu.com/resources.html
[Accessed 9 December 2014].

Lehner, P., Seyed-Solorforough, M. & O'Connor, M. F., 1997. Cognitive Biases and Time Stress in Team Decision Making. *IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems & Humans* , 5 September, pp. 698-703.

Leka, S., Griffiths, A. & Cox, T., 2004. *Work Organization and Stress: Systematic Problem Approaches for Employers, Managers, and Trade Union Representatives. Protecting Workers Health Series No. 3. World Health Organization.* [Online]
Available at: http://www.who.int/occupational_health/publications/pwh3rev.pdf

Macrae, R. R. & John, O. P., 1992. "An Introduction to the Five-Factor Model and Its Applications.". *Journal of Personality 60,,* Volume 60, pp. 175-215.

Manjak, M., 2006. *Social Engineering your Employees to Information Security.* [Online]
Available at: http://www.sans.org/reading-room/whitepapers/awareness/social-engineering- employees-information-security-1686
[Accessed 5 February 2014].

Mitnick, K. D. & Simon, W. L., 2002. *Art of Deception: Controlling the Human Element of Security.* s.l.:John Wiley & Sons.

Mugala, M., 2014. *Social Engineering*, s.l.: s.n.

Mugenda, O. M. & Mugenda, A. G., 2003. *Research Methods Quantitative and qualitative approaches.* Nairobi: Acts Press..

Nebeker, C., n.d. *Basic Research Concepts.* [Online]
Available at: http://ori.hhs.gov/education/products/sdsu/res_des1.htm
[Accessed 26 March 2015].

NIST, 2002. Risk Management Guide for Information Technology Systems. Issue Special Publication 800-30.

Oosterloo, B., 2008. Social Engineer's Motives . In: *Managing Social Engineering Risk: Making Social Engineering Transparent.* s.l.:University of Twente-The Netherlands, pp. 14-15.

Open Web Application Security Project (OWASP), n.d. *CISO AppSec Guide: Reasons for Investing in Application Security.* [Online]
Available at:
https://www.owasp.org/index.php/CISO_AppSec_Guide:_Reasons_for_Investing_in_Application_Security
[Accessed 2 4 2016].

Oso, W. Y. & Onen, D., 2009. *A General Guide to Writing Research Proposal and Report.* s.l.:Jomo Kenyatta Foundation.

OWASP, 2013. *CISO AppSec Guide: Reasons for Investing in Application Security.* [Online]
Available at:
https://www.owasp.org/index.php/CISO_AppSec_Guide:_Reasons_for_Investing_in_Application_Security
[Accessed 2 April 2016].

Pahnila, S., Siponen, M. & Mahmood, A., 2007. *Employees' Behavior Towards IS Security Policy and Compliance.* Waikoloa, Big Island, HW, IEEE 2007.

Parrish, J. J., Bailey, J. L. & Courtney, J., 2009. "A Personality Based Model for Determining Susceptibility to Phishing Attacks. In: Oklahoma City, Oklahoma: Southwest Decision Sciences Institute, pp. 285-296.

Peltier, T. R., 2014. *Social Engineering: Concepts and Solutions.* [Online]
Available at: http://www.infosectoday.com/Norwich/GI532/Social_Engineering.htm#.VO7BgiyzkrM
[Accessed 2 February 2015].

Proofpoint, 2016. *www.proofpoint.com.* [Online]
Available at: https://www.proofpoint.com/human-factor-2016
[Accessed 4 April 2016].

Rohita, S., 2013. [Online]
Available at: http://resources.infosecinstitute.com/social-engineering-a-hacking-story
[Accessed 18 June 2014].

Rouse , M., 2015. *Search Security.* [Online]
Available at: http://searchsecurity.techtarget.com/definition/Pharming
[Accessed 2 March 2015].

Rouse, M., 2014. *Phishing.* [Online]
Available at: http://searchsecurity.techtarget.com/definition/phishing
[Accessed 20 March 2015].

Rouse, M., 2014. *Shoulder Surfing.* [Online]
Available at: http://searchsecurity.techtarget.com/definition/shoulder-surfing
[Accessed 15 March 2015].

Salgado, J., 2002. The Big Five Personality Dimensions and Counterproductive Behaviors.. *International Journal of Selection and Assessment,* Issue 10, pp. 117-125.

Sandouka, H., Cullen, A. J. & Mann, I., 2009. *"Social Engineering Detection Using Neural Networks,".* Bradford, Yorkshire, United Kingdom, s.n.

Sharek, D., Swofford, C. & Wogalter, M., 2008. *"Failure to Recognize Fake Internet Popup Warning Messages" Proceedings of the Human Factors and Ergonomics Society 52nd Annual Meeting.* New York, SAGE Publications,.

Shaughnessy, J. J., Zechmeister, E. B. & Zechmeister, J. S., 2012. *Research Methods in Psychology.* 9 ed. New York: McGraw Hill.

Sheng, S., Holbrook, M., Kumaraguru, P. & Cranor, L., 2010. *"Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions.* Atlanta, GA, s.n.

Shetty, D., 2011. *Social Engineering : what is it, and how to defend yourself.* [Online]
Available at: http://www.itsecurity.be/social-engineering-what-is-it-and-how-to-defend-yourself
[Accessed 21 November 2015].

Social Engineer Inc, n.d. *Security Through Education.* [Online]
Available at: http://www.social-engineer.org/framework/influencing-others/pretexting/
[Accessed 25 9 2015].

Social Engineering Institute, 2014. *Unintentional Insider Threats: Social Engineering.* [Online]
Available at: http://www.sei.cmu.edu
[Accessed 3 July 2015].

Stroud, F., 2016. *Webopedia.* [Online]
Available at: http://www.webopedia.com/TERM/D/dridex-malware.html
[Accessed 3 May 2016].

The Committee of Sponsoring Organizations of the Treadway Commission, 2004. *Ebterprise Risk Management-Integrated Framework "Executive Summary Framework".* [Online]
Available at: www.coso.org
[Accessed 23 March 2015].

University of Illinois, n.d. *Privacy and Information Security :Data Classification Guide.* [Online]
Available at: https://security.illinois.edu/content/data-classification-guide
[Accessed 10 9 2015].

Vishwanath, A. et al., 2011. Why Do People Get Phished? Testing Individual Differences in Phishing Vulnerability within an Integrated, Information Processing Model. *Decision Support Systems,* Volume 51, pp. 576-586.

Webopedia, 2015. *Vishing.* [Online]
Available at: http://www.webopedia.com/TERM/V/vishing.html
[Accessed 21 March 2015].

Weiner, I. & Green, R., 2008. *Handbook of Personality Assessment..* s.l.:John Wiley & Sons,.

Workman, M., 2007. Information Systems Security. *Gaining Access with Social Engineering: An Empirical Study of the Threat, Information Systems Security.*, 16(6).

APPENDIX 1: LETTER OF INTRODUCTION

Macharia Kiama,
P.O BOX, 23335-00100
Nairobi
Cell: 0721946974

To whom it may concern,

RE: SUPPORT ON MSC PROJECT

I am currently a student at the University of Nairobi undertaking a course in Masters of Science in Information and Communications Technology Management. As part of the requirement for graduation, I'm undertaking a study on how to Social Engineering: Managing the human element of security in the context of information system security. In this regard, I'm kindly requesting for your support in terms of time, and by responding to the attached questionnaire. Your accuracy and candid response will be critical in ensuring an objective research, and all information received will be treated in strict confidence.

In addition, the findings of the study will solely be used for academic research purposes. If need be the research report may be presented to the organization for information and record.

Thank you for your valuable time on this.

Yours faithfully,

Macharia Kiama

APPENDIX 2: QUESTIONNAIRE

(Bond, n.d.)

COMPANY NAME	
DATE	

SECTION A: DEMOGRAPHIC INFORMATION

1. What is your position within the company?
    a. Full time employee
    b. Part time employee
    c. Intern
    d. Other

SECTION B: ANTI-VIRUSES & FIREWALLS

2. Have you ever found a virus or Trojan on your computer at work?
    a. Yes, my computer has been infected before.
    b. No, my computer has never been infected.
    c. I do not know what a virus or Trojan is.
3. Is anti-virus currently installed, updated and enabled on your computer?
    a. Yes it is.
    b. No it is not.
    c. I do not know how to tell.
    d. I do not know what anti-virus is.
4. Is the firewall on your computer enabled?
    a. Yes, it is enabled.
    b. No, it is not enabled.
    c. I do not know what a firewall is.

SECTION C: EMAILS

5. When I receive an email, I can rely on the fact that it comes from the person in the "From" address?
    a. False.
    b. True
    c. I don’t know.
6. You receive an attachment which doesn't appear related to work and it is received from someone you do not know. Do you:
    a. Delete the email, since it's probably spam
    b. Open up the email but check out the attachment only if they look interesting
    c. Read the email, but do not open any attachments
    d. Read the email, but don't open any attachments unless you know the sender
7. Do you know what an email scam is and how to identify one?
    a. Yes I do.
    b. No, I do not.
8. The links in emails from unfamiliar sources are generally safe to click on.
    a. True
    b. False
    c. I don’t know
9. My email is private and no one can look at it.
    a. True
    b. False

SECTION D: POLICIES & PASSWORDS

10. In what situations have you ever given your password from work to someone else?
    a. When the boss needed something urgently and I was not around to log in to my account.
    b. When the IT personnel ask for it to configure my account
    c. Never
11. Do you know who to contact in case of an IT security incident?
    a. Yes, I know who to contact.
    b. No, I do not know who to contact.
12. Who is responsible for information security in your department?
    a. Department head
    b. Everyone, including myself
    c. Local IT support staff

13. Do we have policies on which websites you can visit?
    a. No, there are no policies, I can visit whatever websites I want while at work.
    b. Yes, there are policies limiting what websites I can and cannot visit while at work, but I do not know the policies.
    c. Yes, there are policies and I know and understand them.
14. Do we have policies on how what you can and cannot use email for?
    a. No, there are no policies, I can send whatever emails I want to whomever I want while at work.
    b. Yes, there are policies limiting what emails I can and cannot send while at work, but I do not know the policies.
    c. Yes, there are policies and I know and understand them.
15. Is instant messaging allowed in our organization?
    a. Yes, instant messaging is allowed in our organization.
    b. No, instant messaging is not allowed in our organization.
    c. I do not know.
16. Can you use your own personal devices, such as your mobile phone, to store or transfer company information?
    a. Yes I can.
    b. No I cannot.
    c. I do not know.
    d. Yes I can, if using the company provided solution.
17. When constructing your password you should:
    a. You should use your family member name, favorite sports team or year of birth
    b. Use phrases or mispelled words embedded with numbers and special characters
    c. Use sequenced numbers and letters fom your keyboard.
    d. All the above.
18. Do you use the same passwords for your work accounts as you do for your personal accounts at home, such as Facebook, Twitter or your personal email accounts?
    a. Yes I do.
    b. No I do not.
19. Have you logged into work accounts using public computers, such as from a library, cyber café or mall?
    a. Yes, I have
    b. No, I have not
20. What is one of the ways that you can secure your password from disclosure?
    a. You can write it down on a sticky pad and stick it on your monitor
    b. You can write it down only if you keep it in a secure place like your wallet without header information. Password should “NOT” be kept in a computer file
    c. Save it on your mobile phone for quick access
    d. All the above

SECTION E: GENERAL SECURITY QUESTIONS

21. Do we have an information security team?
    a. Yes, we have a company security team.
    b. No, we do not have a company security team.
    c. I do not know.
22. Would you recognize an IT security incident on your computer if you saw one?
    a. Yes, I know what to look for.
    b. No, I do not know what to look for.
    c. Not sure
23. If you format a hard drive/flashdisk or erase the files on it all the information on it is Permanently lost.
    a. True
    b. False
    c. Don’t know
24. Is your computer configured to be automatically updated?
    a. Yes, it is.
    b. No, it is not.
    c. I do not know.

25. What in your opinion is the largest source of risk to your department's information security?
    a. Computer viruses and other "malware"
    b. Defective software
    c. Defective hardware
    d. Human mistakes, malicious or otherwise
26. How often do you take information from the office and use your computer at home to work on it?
    a. Almost every day.
    b. At least once a week.
    c. At least once a month.
    d. Never
27. Have you received an email, call or s.m.s. within the past 6 months that you suspect was an attempt to get your personal details for fraudulent purpose?
    a. Yes
    b. No
    c. I don't know
28. Do you have a method to validate your bank or mobile phone service provider when they call/text e.g. M-Pesa?
    a. Yes
    b. No
    c. I don't know
29. How do you get rid of your information such as bank statements?
    a. Bin it
    b. Shred it
    c. Keep it
30. Have you heard the term "phishing" before?
    a. Yes
    b. No
31. Have you heard the term "Social Engineering" before?
    a. Yes
    b. No
32. What do you think it means if you have answered "Yes" above?
    a. Engineers working socially
    b. Method used by malicious people to get information
    c. A study of social science
33. You notice someone in the office you do not know. What do you do?
    a. Ask them if they're lost, and give them directions if needed
    b. Ask them to identify themselves and escort them to their meeting
    c. Leave them alone if they don't appear lost. If they need help, they will ask
    d. Verify with whoever they have come to see whether they were expecting them
34. Do you think it is necessary to call a company to verify the identity of its employee if presented with an ID card?
    a. Yes
    b. No
    c. I don't care

THE END. THANK YOU!!