UNIVERSITY OF NAIROBI

School of Computing and Informatics

INFORMATION SECURITY AWARENESS MEASURING MODEL - A CASE STUDY OF NAIROBI STOCK EXCHANGE SYSTEMS

NDUNG'U, RICHARD MWANGI

P54/65341/2013

Supervisor: Dr. Evans Miriti

PROJECT REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE DEGREE OF MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

JUNE 2014

Declaration

This research project as presented on this report is my original work and has not been presented for any other University award.

Signed: ……

Date: ……

Ndung'u. Richard Mwangi

This research project has been submitted as part of fulfillment of the requirement for Masters of Science in Information Technology Management of the University of Nairobi with my approval as the supervisor.

Signed: ……

Date: ……

Dr. Evans Miriti

Abstract

Information Security awareness initiatives are seen as critical to any information security programme. Organizations are highly dependent on information management and processes and this creates a level of security alert. Statistics show that most security breaches are the result of insider misconduct, as opposed to hacking by outsiders. Often this insider misconduct is the result of ignorance rather than malfeasance. (Rhodes, 2015)

It is therefore important to train users on the importance of information security and follow the policies that are in place to protect that data from theft, loss or damage. This training creates another level of defense for an organization.

The research problem was that despite the fact that NSE conducted information security awareness programs to its users; there was lack of a model to measure whether the information security awareness was at an acceptable level on its users. This was deemed to be the weakest link in this security control measure.

The objectives of this research were to; establish techniques used to impart information systems security awareness and their effectiveness and also to establish the extent to which NSE measure their information systems security awareness levels.

However, the main question was how to determine the effectiveness of these awareness initiatives. Does awareness training have a direct influence on the security behavior of individuals, and what is the direct benefit of awareness training?

The research presented a theory-based literature review of the approaches used within Nairobi Stock Exchange Automated Trading System users' on information security awareness. And to what extent does information security awareness training influence information security behavior?

From the validations, it can be stated that the study was a success. Further study on the field is highly encouraged to explore other possibilities in this field of Information Security awareness.

Acknowledgement

I wish to express my sincere appreciation to Dr. Evans Miriti, my supervisor for his invaluable counsel and guidance towards the successful completion of this research project, and indeed for his immense assistance all through this Masters of Science course.

I am also indebted to Prof. Wagacha, Prof. Omwenga and Mr. Ruhiu for the guiding me during all stages of this project. I cannot forget the whole School of Computing fraternity for their invaluable support and most notable being the Librarian Nancy.

In addition, I owe my thanks to my immediate and extended family for their love, encouragement and inspiration.

And above all, I wish to thank the Almighty GOD.

Thank you.

Dedication

This research project is dedicated to the love of my life, the corner stone of my family; my dear wife Purity and to my two adorable kids; my son Alex and my daughter Joan for giving me a chance to be a role model and for inspiring me towards further studies.

List of Figures

List of Tables

Acronym and Abbreviations

ATS - Automated Trading System

NSE - Nairobi Securities Exchange

SPSS - Statistical Package for the Social Sciences

CDSC - Central Depository and Settlement Corporation

CMA - Capital Market Authority

I.T - Information Technology

ICT - Information and Communication Technology

COSO - Committee of Sponsoring Organization

FTSE - A share index of the 15 and 25 companies listed on the Nairobi Securities Exchange with the highest market capitalization

OPF - Open Process Framework

T+3 - Transaction day plus three more days

T+4 - Transaction day plus four more days

WAN - Wide Area Network

BBO - Broker Back Office

AHP - Analytic Hierarchy process

Table of Contents

1. INTRODUCTION

1.1 Background

Nairobi Securities Exchange (NSE) is an organization which dates back in the 1920s during the colonial times. It started as an informal market which had no rules and regulations to govern stock broking activities. Trading simply took place on a 'gentleman's agreement' and standard commissions were charged with clients being obliged to honor their contractual agreement. However, this was formalized in 1953 in collaboration with London Stock Exchange through the establishment of the first stock broking firm Drummond Stock brokers. (NSE, Nairobi Securities Exchange History, 2014).

The Capital markets in Sub Saharan Africa, Kenya included displayed extreme thinness and illiquidity compared with other emerging markets of South East Asia (Ziorklui, 2001). In 1986, The Government of Kenya made a deliberate policy effort to foster growth of the Capital Markets through adoption of The Sessional paper No.1 of 1986, which recognized the Capital markets as key in achieving meaningful economic growth and development.

Today, NSE constitutes of eighteen Stockbrokers and Investment Banks. And since NSE was formalized, trading was done through the auction on the floor, where a maximum of two dealers from each broker were present on the floor from 9.30am to 1pm when the auction commenced and ended respectively. Auction was done through 'shouting of the buy or sell orders'. Trading was conducted by the Central Depository and Settlement Corporation (CDSC). After every trading day, the share certificates issuance were lounged through the registrar of companies, for the issuance of share certificates after five working days.

In July 2011, the Nairobi Stock Exchange Limited changed its name to the Nairobi Securities Exchange Limited. (NSE, Nairobi Securities Exchange History, 2014) The change of name reflected the strategic plan of the Nairobi Securities Exchange to evolve into a full service securities exchange which supports trading, clearing and settlement of equities, debt, derivatives and other associated instruments. In the same year, the equity settlement cycle moved from the previous T+4 settlement cycles to the T+3 settlement cycle. This allowed investors who sell their shares, to get their money three (3) days after the sale of their shares. The buyers of these stocks will have their CDSC accounts credited with the shares, in the same time.

In September 2011 the Nairobi Securities Exchange converted from a company limited by guarantee to a company limited by shares and adopted a new Memorandum and Articles of Association reflecting the change.

In October 2011, the Broker Back Office (BBO) commenced operations. (NSE, Nairobi Securities Exchange History, 2014) A Broker Back Office is a system, designed to help the broker to manage all the NSE business requirements. The system has the capability to facilitate internet trading which can improve the integrity of the Exchange trading systems can facilitate greater access to the securities market.

NSE ATS most notable feature is that, it can execute the trading strategy when the trading auction goes live. Essentially, it's a rules driven software system. The trader can select from the many of historical indicators representing the stocks' previous conditions. The indicators should be updated daily using the latest data. They take the emotion out of investing. The program also has a manual override so the stock trader can manually place a trade order as well. But basically, the most exploited function of this feature is the stock trader placing the trade orders manually.

Other features on this NSE ATS are:

i. Alerts – setting up personalized alerts for portfolio.
ii. Conditional Orders - You can place orders that, when executed, immediately triggers or cancels another orders.
iii. Quick Order Entry - You have the option to quickly enter or cancel orders faster than normal.
iv. Real-Time Charts - The broker offers access to charting tools that update in real time.
v. Spread Builder - The broker offers a tool to build your own spreads between multiple investment products.
vi. Trailing Stops - You can set a stop-loss as a percentage below the market price that adjusts as the price fluctuates to help you secure profits and cut losses.
vii. Watch List - You can create watch lists to keep an eye on investment products that interest you.
viii. Export Data - You can export your portfolio or account statements.

In November 2011 the FTSE NSE Kenya 15 and FTSE NSE Kenya 25 Indices were launched. The launch of the indices was the result of an extensive market consultation process with local

asset owners and fund managers and reflects the growing interest in new domestic investment and diversification opportunities in the East African region.

As of March 2012, the Nairobi Securities Exchange became a member of the Financial Information Services Division (FISD) of the Software and Information Industry Association (SIIA).

In March 2012 the delayed index values of the FTSE NSE Kenya 15 Index and the FTSE NSE Kenya 25 Index were made available on the NSE website www.nse.co.ke. The new initiative gave investors the opportunity to access current information and provides a reliable indication of the Kenyan equity market's performance during trading hours (NSE, /about-nse/history-of-organisation.html, 2014)

1.2 Problem Statement

Information is one of the resources that Nairobi Securities Exchange is heavily dependent on to achieve its mandate. If the critical information of the organization is compromised, the Stock exchange is likely to suffer serious consequences, that is, in the form of loss of income, loss of customers' trust and maybe legal action among other consequences. Therefore, information should be protected and secured.

Information security awareness is about guaranteeing that all employees at different levels of ATS usage are aware of the rules and regulations regarding securing the information within organization.

Information security awareness should therefore form an integral part of any organizations' overall information security management plan.

Threats to organizations and information systems are increasing in occurrence and in complexity and this emphasize the urgency for organizations to learn how to better protect their information and information systems (Schneier, 2004).

Sipior & Ward, states that automations has brought with it escalation of concerns which include consumer confidence in outline business activities, threat to data integrity, legal liability and possible suffering of a financial loss. (B.T, 2008)

NSE conducts information systems security awareness programs to sensitize their staff on the main information systems security risks facing the ATS and the associated control measures. This is done because of the knowledge that even in the presence of software and hardware

controls, in the absence of appropriate levels of information security awareness, these users could potentially be the weakest link in the information security process.

There is no evidence that research has been carried out to determine the information security awareness levels of NSE's ATS users and it is for this reason that there is need to thoroughly assess and propose a solution.

1.3 Research objectives

The main objective of this research is to focus on the measurement of Information Security awareness levels with a view of proposing an information security measuring model that can be utilized by the Nairobi Stock Exchange. This research also touches on review of how awareness activities are carried out as well as the effectiveness of those awareness activities.

The specific objective of this research is to:

i. Establish techniques used to impart information systems security awareness and their effectiveness.
ii. To assess user level of awareness in anticipating the risk.
iii. Establish the extent to which NSE measure their information systems security awareness levels.
iv. Establish the security of ATS users' data and what measures have been put in place by the Nairobi Stock Exchange.
v. Develop a security awareness measurement model that can be adopted by the Nairobi Stock Exchange.

1.4 Research questions

The study is focused on finding the information security awareness of NSE ATS users' in the newly introduced automated trading system. Therefore the research seeks to answer the following questions:

i. How does NSE measure their information security awareness levels?
ii. How does NSE carry out their information security awareness and how effective are they?
iii. Which Information security awareness measurement model can be used effectively in the Nairobi Stock Exchange?
iv. What information security controls can be put in place to mitigate or eliminate possible information security risks facing the automated trading system?

1.5 Significance of the Study

This study will be a critical point of reference from stock market investors, scholars, the NSE, CMA and CDSC boards.

i. Scholars will benefit in that they can use the references and findings from this study to do further research on this topic of automated trading systems.
ii. The study will identify the level of users' awareness and knowledge of the information security in the Automated Trading System.
iii. The NSE, CDSC and CMA boards would also benefit from the results of this evaluation of the Automated Trading System (ATS) in Kenya, and probably take note of some of the critical points that may arise out of the study.

1.6 Scope

The scope of our research is confined on the entities that comprise the Nairobi Security Exchange. These include the Stockbrokerage firms, Investment banks and Unit trust firms as well as the NSE watchdog The Capital Market.

2. LITERATURE REVIEW

2.1 Introduction

Oxford Online Dictionary defines Security as; 'the state of being free from danger or threat'. It also further defines security as 'the degree of resistance to, or protection from, harm. It applies to any vulnerable and valuable asset, such as a person, dwelling, community, nation, or organization'.

Merriam-Webster Dictionary describes security as "Freedom from danger". Going by this simple definition, we can say that there is no completely secure system, if danger is always around us. And according to (Kearney K. , 2005), Information Security awareness is a dynamic and ongoing process made more complex by risks that are continuously adapting to the current environment.

The protection of the confidentiality, integrity and access to information is referred to as information security (Kruger and Kearney, 2006). Evidence indicates that, organizations will still undergo security breaches in spite of the amount of technical controls in position (Arief, 2005).

2.2 Background of Automated Trading System (ATS)

An automated trading system (ATS) is a computer trading program that automatically submits buy and sell instructions to an exchange, (Andreas Charitou, 2009). An early ATS is Instinet which allowed traders to input orders invisibly to the market, with a crossing price determined by a Volume-Weighted Average Price (VWAP); the ratio of the value traded to total volume traded over a particular time horizon (usually one day); which is a measure of the average price a stock traded at over the trading horizon. Instinet also enables anonymous conversations and negotiations to take place between bidders, and so reduces informational costs to the participants (Jiang et al, 2001).

ATS operations may provide benefits to the marketplace. Depending on the system involved, some of the potential benefits include lower costs, specialized services, ease of access, and expanded product ranges. However, ATS operations may also raise concerns, such as the fitness and properness of the system operator, lack of transparency, adequacy of surveillance arrangements, and the maintenance of security and control procedures and back-up arrangements. Automated trading system forms an excellent starting point for everyone who is interested in turning the stock market opportunities into considerable profit (Venkataraman, 2001)

In 2006, the Automation of trading at the NSE was implemented through the Automated Trading System (ATS). And in the year 2007, Wide Area Network (WAN) ATS was introduced and this made it possible for brokers to buy and sell stocks from the comfort of their offices without the need of going to the NSE auctioning floor.

2.2.1 Drawbacks of an Automated Trading System

i. ***Mechanical* failures**

Although it would be great to turn on the computer and leave for the day, automated trading systems do require monitoring. This is due do the potential for mechanical failures, such as connectivity issues, power losses or computer crashes, and to system quirks. It is possible for an automated trading system to experience anomalies that could result in errant orders, missing orders, or duplicate orders. If the system is monitored, these events can be identified and resolved quickly.

ii. ***Security Breaches***

ATS operations may raise concerns; lack of transparency, adequacy of surveillance arrangements, and the maintenance of security and control procedures and back-up arrangements.

According to Automated Trader (Trader, 2014), defending automated trading systems is usually done in one of two ways:

- **Physical security -** The system is secured by isolating the systems to be protected from cyber-interaction.
- **Simplified lock-down -** Security is achieved by minimizing access rights to a few privileged employees with high security clearances/special permissions.

2.3 Automated Trading System Security

Automated trading system security theory as defined by the author (Yen-Ping Ch, 2003) could be expressed in the following functions:

Information security: information security policy, risk management, internal control, information auditing, contingency management.

Internal control: personnel security control, physical security control, systems and network security control, access control, system development and maintenance control, business continuity management.

Contingency management: environment inside or outside of an organization, information management, information techniques.

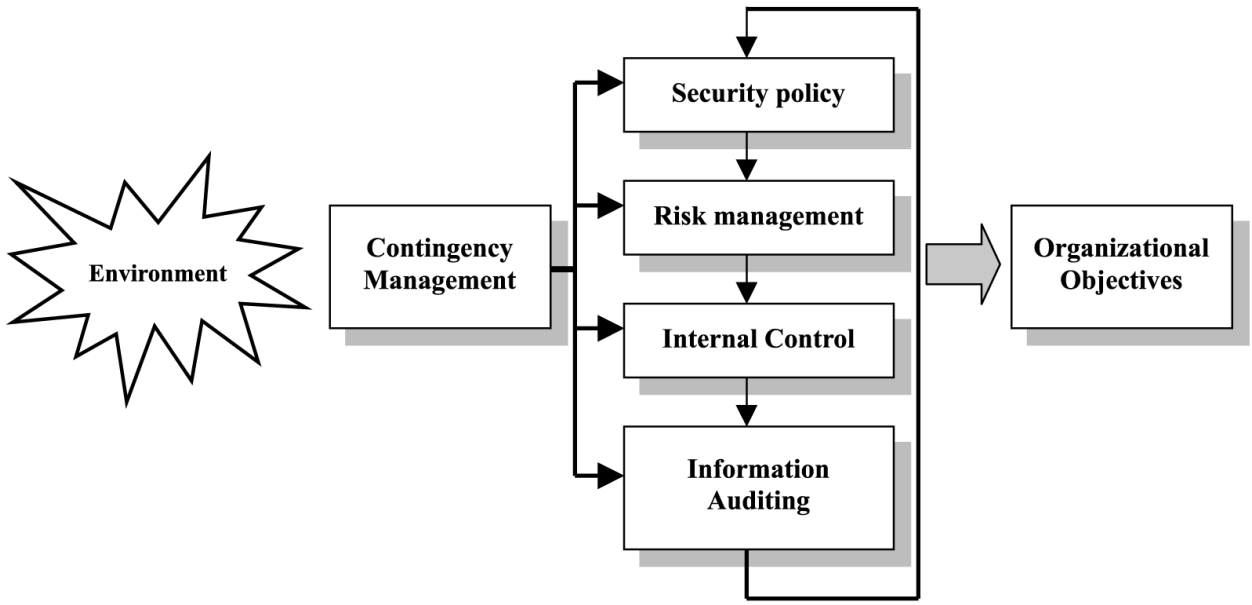


Fig. 1: A diagrammatical illustration of integrated system theory (Hong, 2006)

2.3.1 Contingency Management

For contingency theorists, information security management is a part of contingency management that is meant for the prevention, detection and reaction to the threats, vulnerabilities and impacts inside and outside of an organization. To meet the demands of a fast-changing environment, it is reasonable for practitioners to take on one or more information security management measures, for example security policy actions, risk management actions, control and auditing actions or system management actions

Contingency management leads to preparedness in the event of an emergency, disaster, or system failure. It utilizes risk assessment and is intended to identify vulnerabilities and threats, and to implement countermeasures to prevent an incident or limit its impact should it occur. Planning for operational continuity and disaster recovery are key components of contingency management. (smallbusiness)

i. **Purpose**

Some business resources and functions are critical to an organization's success and continued operations. Therefore, it is essential that an organization's processes operate effectively without excessive interruption. Contingency management supports this objective through the creation of plans, procedures and technical measures that can enable the efficient recovery of business operations following a business disruption or disaster.

ii. **Vulnerability**

The identification of vulnerabilities is a vital step in contingency planning and the implementation of countermeasures that prevent an incident or limit its impact if it does occur. Vulnerability is a weakness in a system, a security procedure or internal controls, which can be exploited by a threat source. Some vulnerability can be eliminated or minimized through operational or technical solutions specified in a contingency plan. However, it is not possible to eliminate all risks.

iii. **Threat**

Contingency management requires the identification of threats. A threat may take the form of a natural event such as a flood, tornado, earthquake or hurricane, or it may assume a technical or man-made form that may be radiological, chemical, biological, mechanical or electrical in nature. A threat may also be an intentional act such as an act of terrorism, a demonstration, a bomb, assault, theft or a computer incident.

iv. **Contingency Planning**

Contingency planning identifies interim measures to respond to threats and recover from a business or system disruption. Such measures may involve the relocation of operations and IT systems to an alternate site; the recovery of functions using alternate equipment and personnel; or the reliance on manual rather than technical methods to perform critical functions. Contingency planning requires the creation of plans and procedures and the identification and

implementation of technical measures that will enable the recovery of business processes, IT systems and data following a business disruption.

2.3.2 ICT Security Policy

Security awareness is the knowledge and attitude members of an organization possess regarding the protection of the physical and especially, information assets of that organization. Many organizations require formal security awareness training for all workers when they join the organization and periodically thereafter, usually annually (Lebek, Uffen, Breitner, & Neumann, 2013).

Vesta Technology Solutions describes Security policy as; a document that states in writing how a company plans to protect the company's physical and information technology (IT) assets (Solutions, 2015) A security policy is often considered to be a "living document", meaning that the document is never finished, but is continuously updated as technology and employee requirements change (Rouse, 2007)

A security policy establishes what must be done to protect information stored on computers. A well-written policy contains sufficient definition of “what” to do so that the “how” can be identified and measured or evaluated. An effective security policy also protects people. Anyone who makes decisions or takes action in a situation where information is a risk incurs personal risk as well. A security policy allows people to take necessary actions without fear of reprisal. Security policy compels the safeguarding of information, while it eliminates, or at least reduces, personal liability for employees (Bowden, 2003)

A security policy is a documented strategy on protecting and maintaining availability to a network and its resources (Christopher Budd, 2015). Listed below are some areas that the NSE ICT policy document covers:

i. ATS use Policies
ii. Risk Assessments
iii. Password Policies
iv. Administrative Responsibilities
v. User Responsibilities
vi. Internet Policies
vii. Disaster Recovery (Backup and Restore)

viii. Intrusion Detection

The following are some of the areas that should have been included in the Policy document:

i. Electronic Communication with traders Policy and Procedure
ii. Institutional Planning Policy and Procedure
iii. Policy and Procedure Framework
iv. Privacy Policy
v. Procurement and Purchasing Policy and Procedure

2.3.3 Risk Management

Economic Times defines risk management as; 'the practice of identifying potential risks in advance, analyzing them and taking precautionary steps to reduce/curb the risk'. (Times, 2015)

The diagram in fig. 2 represents the core components of a risk management process model based upon an open process framework (OPF) (professionals., 2014).

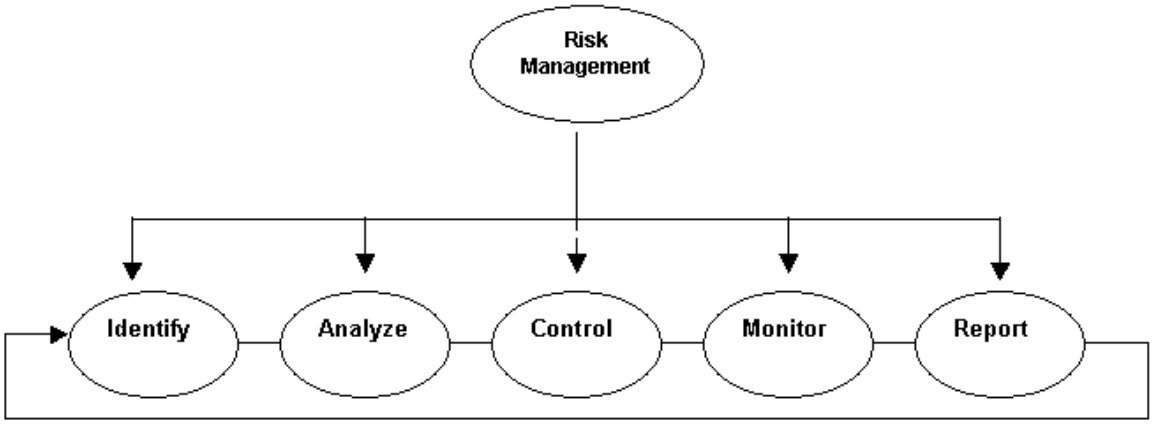


Fig 2: Core components of a risk management process model based upon an Open Process Framework (OPF) (Landess, 2003)

i. Identify - The identification of an event that may cause information risk.
ii. Analyze - The assessment, measurement and prioritization of threats and vulnerabilities to information for the purpose of selecting information security controls.
iii. Control - A policy, method, procedure or mechanism that addresses identified threats and vulnerabilities to information resources.
iv. Monitor - The process of systematically evaluating the organization by measuring the performance of information controls in order to initiate remedial action.

v. Report - The process of systematically reporting to decision makers an accurate, comprehensive and coherent assessment of information risk.

2.3.4 Internal Controls

Compass Point, describes internal controls as a set of policies and procedures to prevent deliberate or misguided use information/funds for unauthorized purposes. Internal controls are fundamental to achieving key initiatives and goals. An organization should establish the access control — the doorway to all IT systems and corporate resources. Access controls specify how the business will monitor its IT resources and how they should be used. The most commonly used access controls include user accounts, consisting of passwords and usernames; login and resource access rights; and the establishment of privileged system accounts (Point Compass, 2014).

Internal controls are designed to assist organizations in achieving their objectives. According to COSO framework (Rittenberg, 2009), the five components of internal control are risk assessment, control environment, control activities, Information and communication and monitoring.

In their 2012 *Internal Control Guidelines Report* (CMA, 2012), states that; 'there should be continuity/disaster recovery plans existing for all NSE IT monitoring and reporting systems. And there should be established a system of communication for individuals to report suspected breaches of laws or regulations the trading at the NSE ATS. The same report further states that the management shall ensure that key components of the information management system design and implementation programme are adequately documented and regularly reviewed for effectiveness. And that, the Management shall ensure that appropriate and effective data security policies and procedures are implemented to prevent and detect the occurrence of errors, omissions or unauthorized insertion, alteration or deletion of, or intrusion into, the data processing system of the firm (electronic or otherwise) and data (covering all confidential information in the possession of the firm, such as clients' personal and financial information and price sensitive information).

2.3.5 Information Auditing

An information technology audit is an examination of the checks and balances, or controls, within an information technology (IT) group. An IT audit collects and evaluates "evidence" of an organization's information systems, practices, and operations. According to About.com, the

evaluation of this evidence determines if the information systems are safeguarding the information assets, maintaining data integrity, and operating effectively and efficiently to achieve the organization's business goals or objectives. (About.com, 2014)

Information technology audits are used to evaluate the organization's ability to protect its information assets and to properly dispense information to authorized parties. The IT audit aims to evaluate the following:

i. Will the organization's computer systems be available for the business at all times when required?
ii. Will the information in the systems be disclosed only to authorize users?
iii. Will the information provided by the system always be accurate, reliable, and timely?

2.4 Comparison of existing models to measure awareness levels in organizations

2.4.1 The Kruger and Kearney perspective

Kruger and Kearney, developed a model that focused on identifying the main aspects of security risks that need to be addressed by the awareness programme, educating the staff on the identified risks and then measuring the impact of their training on their staff, their knowledge and practice of the same (Kruger and Kearney, 2006). An evaluation of six specific risks is highlighted as the ones that will be focused on in the awareness initiative. While this came with a wide variety of awareness material, only the material regarding the risks identified was used. Some of the content was also modified to fit in with the organization specific needs.

Use of quantitative measurement of security awareness levels is touted as the best in order for security awareness programs to add value to an organization it is necessary to use a structured approach to study and measure its performance (Kruger and Kearney, 2006). The approach utilized by (Kruger and Kearney 2006), opted to classify the areas to measure into dimensions of knowledge. The first dimension focuses on knowledge focusing on what the user knows, attitude focusing on the users thoughts and the users behavior focusing on the users actions.

2.4.2 The Zakaria and Gani Perspective

Zakaria and Gani propose a conceptual information security culture checklist. Due to the dynamism of Information Security, the authors term their list as conceptual since it is bound to be changed and updated constantly (Zakaria, 2003). The objective of the conceptual checklist is to assist the management to implement an information security culture and raise awareness

among an organizations staff about the securing of information. The same checklist can be used as a metric to establish how aware users of an organization are regarding their Information Security.

2.4.3 The Tessem and Skaraas perspective

According to (Skaraas, 2005), organizations should also consider measuring the level of their in-house information security culture. In this case, the term culture analyses user behavior in deeper terms than simply being aware of what is required of a user in terms of Information Security. They are of the opinion that it is difficult to provide empirical data on information security and it is also difficult to make an accurate analysis of information security awareness. However they propose a few metrics that can be used to establish the level of awareness of staff in a particular organization such as the percentage of an organizations staff who have completed awareness training; the number of reported information security incidents; how many staff member leave confidential Information on their Desks and the percentage of lost passwords.

2.5 Information Security Awareness Model Measurement review

2.5.1 Process models in security awareness research

In a conference paper, Hansche stated that information security awareness is the central subject of research and discussed the formation of a process as a collection of events in order to achieve the security goal, which may differ according to the applied context. The central subject and its attributes may alter over time so that the "…awareness program must remain current" (Hansche, 2001). None of the suggestions she makes can on an individual basis result to the specified goal of the process and the sequence of events is important; therefore the model is sequential. She also argues that "they [the security awareness program goals] should reflect and support the overall mission and goals of the organization"; therefore predictability is not achievable. As a consequence, (Hansche, 2001) approach is purely a process one (Cynthia Irvine, 2005), present a series of constraints and barriers to effective security awareness. Their model implicitly involves events, such as the need to first "attract the attention of senior executives towards a common understanding on the rationale and importance of introducing security awareness programs". These events, although not presented in a chronological order are sequential; e.g. they first suggest attracting top management support and in sequel recognize the heterogeneous audience

and their various needs for such a program. Finally, the predictability dimension is negative. Therefore their research model is a process one, as well.

(Peltier, 2005), also describes a framework that focuses on events that contribute in achieving the specified security awareness goals which may change over time, whereas a sole event is not sufficient for achieving these goals. He suggests that earlier events, such as risk analysis, risk assessment, policies, procedures etc. are important for security awareness; therefore organization's context and history are considered as determinant. The sequence of events is also important and the focus is to provide guidelines (not to predict) for effective security awareness programs. (McCoy), describe a framework for establishing a security awareness program. Their approach focuses on events, such as the definition of the program's goals, the determination of the content etc. Their model is sequential since a number of events that should occur in an order are presented. Finally, the dimension of predictability is non-existing, since no attempt of predicting results is made. Therefore, this is another pure process approach.

Finally, a purely process perspective is also adopted by (Spurling, 1995). He suggests that information security awareness is a process that should fit in with the culture of the organization. In order to describe the information security awareness process he sets forth in a narrative way the organization's historical conditions and events which led to the need for security awareness program and map the current state of the organization. These conditions are critical in the security vision and goal definition. The sequence of the historical events and the processes stages are important for the accomplishment of the security awareness goal. His goal is to describe a framework of events that contribute to achieving user's commitment to security, without being able to fully determine them.

2.5.2 Variance models in security awareness research

Many research studies focus on proposing theories or mechanisms that promote 'good' user's behaviour regarding information security (Stanton, 2003). Their methodology includes a desirable outcome or the dependent variable, which is the good end-user behaviour or attitude. The variance model explains outcomes as the product of independent variables acting on dependent variables. As recorded by, (Stanton J.M., 2005), it aims at "promoting good end user behaviours and constraining bad end user behaviours" by developing a taxonomy of end user behaviours and provide practices that promote the desired categories of behaviour. The concepts used are non-temporal variables and the model proposed aims at predicting end-user behaviours.

Therefore, it can be characterized as a pure variance model. (Kearney K. , 2005), aim at assessing information security awareness. Their model lies on non-temporal variables (knowledge, attitude, behaviour and awareness) that are measured through the use of a proposed questionnaire. Causal relationships among the variables are created and predicting increased levels of awareness is the goal of the model. Therefore, their approach is purely variance.

Table 1.0: Assumptions of variance model based on (Engleman, 2004)

Variance model
The entity under study is characterized by a fixed set of variable attributes.
Each variable is treated as though it has the same status or meaning throughout the process.
Any significant change is captured by the variables.
a. Research seeks for causal explanations of the way the independent variables influence the dependent variable. b. The cause is necessary and sufficient for the outcome.
Outcome will invariably occur when necessary and sufficient conditions are present.
The time order in which the variables influence the dependent variable makes no difference.
Explanations capable of generalization over broad range of contexts.

2.6 Security Awareness Prototype

(H.A. Kruger a, 2006), developed a prototype model for measuring information security awareness in an international gold mining company. They measured the effectiveness of information security awareness program on the basis of knowledge, attitude and behaviour.

The prototype presented the researchers with the basic problem regarding what to measure and how to measure in order to gain organizational awareness levels. Basing their model on what to measure, the researchers chose to focus on attitude, behaviour and knowledge as the main factors to measure.

They initiated an information security awareness program. The program involved the following.

A comprehensive toolkit was purchased from a vendor and detailed development of the program started in mid 2003.The first priority was to narrow the focus of the program into a manageable size. After careful deliberation and following a risk elimination process, the program was focused on six critical risk areas or ‘Golden Rules’.

Table 1.1: Kruger and Kearney awareness program

1	Always adhere to company policies
2	Keep passwords and personal identification numbers (PINs) secret
3	Use e-mail and the Internet with care
4	Be careful when using mobile equipment
5	Report incidents like viruses, thefts and losses
6	Beware, all actions carry consequences

The model was then designed to work with regions in mind as the factors that will lead to overall awareness levels. The regions would carry different weights based on their standing within the organization. Each region would have to be evaluated based on a number of factors. The factors were then identified and organized in a structured process through a hierarchy of criteria using a tree structure. A tree structure commonly known as a value tree is formed by starting with an overall objective. The objective may be a complex problem or scenario that is collapsed into several smaller problems. Factors that feed into the smaller general problems are factored in to model. They identified the following main factors to measure as knowledge, attitude and behaviour. The smaller concepts that feed into the main factors were selected by consensus by the researchers with input from the management of the organization for whom the prototype was developed and tested for.

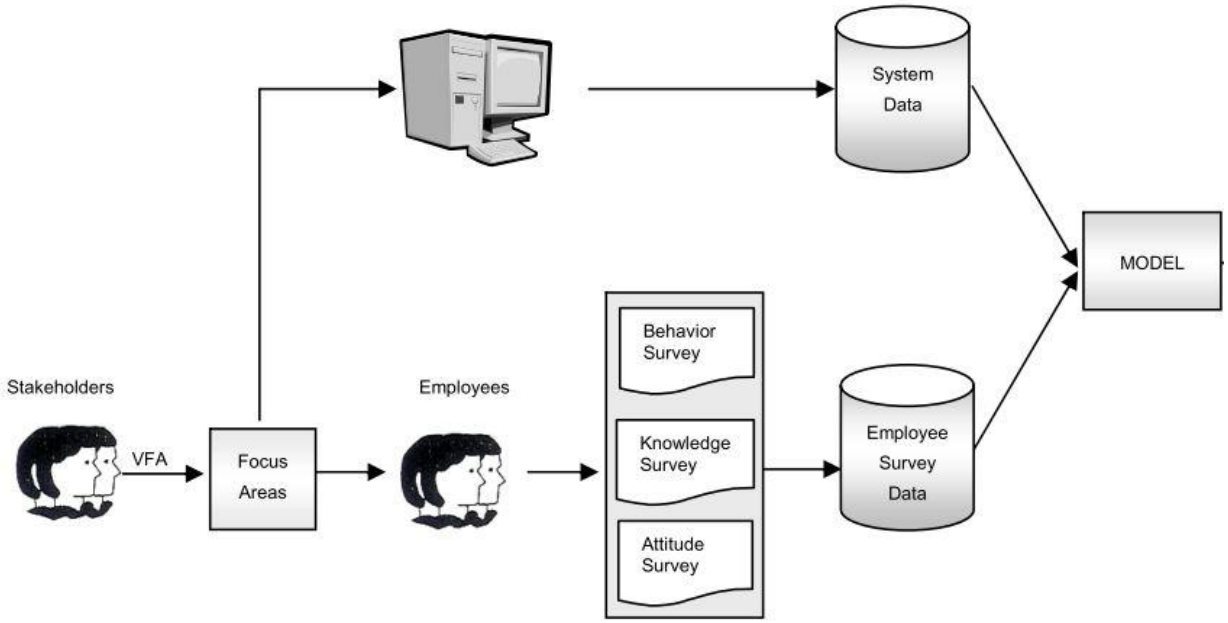


Fig. 4.18: Schematic Kruger and Kearney Security Awareness Prototype Model (Kearney K. a., Information Security Awareness and Culture, 2006)

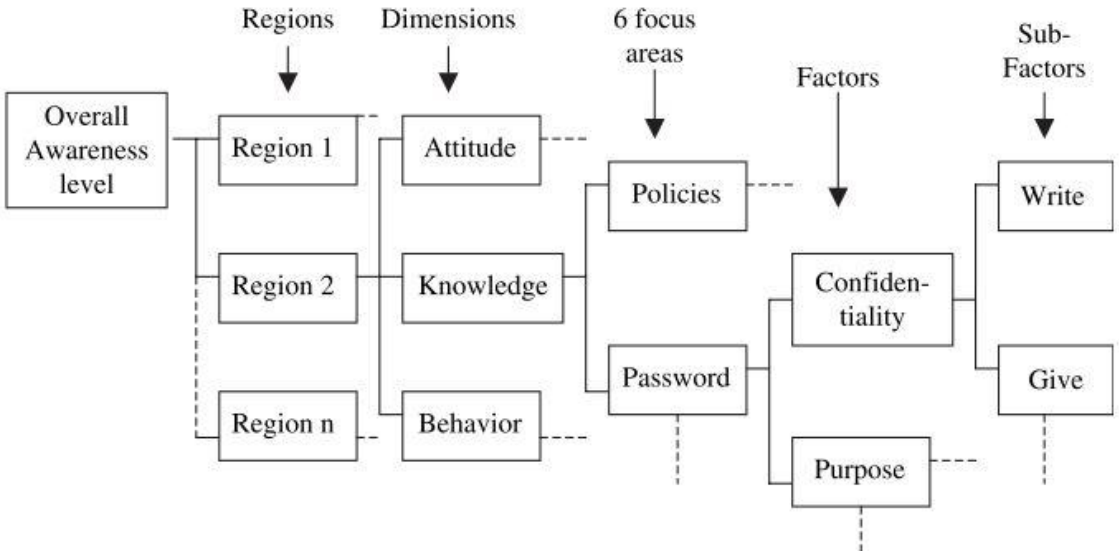


Fig 4.19: Tree Structure of Problem (Kearney K. a., Information Security Awareness and Culture, 2006)

The researchers utilized an off-the-shelf tool that was customized to suit their specific requirements hence some sections of the tool remained unutilized. The researchers developed a program that involved whose core components were as shown in the table below.

The next most critical step was to do an evaluation test. A measuring tool that was robust enough was required to measure the awareness levels within the organization. The challenges faced during the selection and adoption of a measuring tool included the following according to (Kearney K. , 2005):

i. Sustainable
ii. Simplicity
iii. Use of scientific methods to meet the organizations specific needs

The following variables; knowledge, attitude and behaviour would be measured across all the regions although with different weightings for different regions. A thirty five questions questionnaire was used largely focusing on the 6 main areas and factors and sub factors below them. Most of the responses required were in the line of true, false and don't know while others were simply true and false. Since the value tree was designed from a top down approach where the larger problem was broken down to smaller problems, the evaluation would start from the opposite direction whereby the tree will be updated from the lowest value leading all the way to the top to achieve the global value i.e. Organization level awareness.

The measuring mentioned above was done through a scorecard approach which is also referred to as an additive model. The process of allocating different weights to different regions and factors/sub factors was done via a process known as Analytic Hierarchy process (AHP). By utilizing the combined experience of managers of the organization and a preference scale, the researchers were able to allocate the weightings accordingly.

An overview of (Kearney a. K., 2005) prototype the following were listed down as the future development aspects:

i. Fully comprehensive bank of Questions to be developed - The models success is dependent on the right questions being asked by the researcher. The questions also needed to cover as wide an area in Information Security as possible. Another advantage of having a bank of questions is that it enables the organization to give different questions

to different staff in different regions in a random manner hence avoiding the aspect of staff discussing answers due to the exam having the same set of questions.

ii. Weightings - By working with the appropriate management, effective weightings based on the organization needs can be used to come up with effective and representative figures that will accurately describe the awareness levels of the organization in the end.

iii. Use of Practical data - The use of Metrics was not included in the prototype. The metrics would be easy to get data such as number of security incidences, number of awareness trainings etc.

iv. Automation - the process of collecting all the information should be automated in order to make it more effective and less time consuming. The tool can be controlled from a central point and access granted to all the regions across the business.

2.6.1 Limitations of the Kruger and Kearney prototype

Kruger and Kearney Prototype is a representative model which with minor modifications can be applied in any organization that has the objective of measuring Information Security awareness levels. (Kearney K. , 2005) Despite the detailed and quite representative nature of the model, a few limitations exists that need to be highlighted accordingly.

i. The lack of individual level awareness levels within the prototype according to the researcher was one of the limitations of the prototype. The prototype mainly focused on the overall awareness levels of the organization. This is a limitation with minimal impact since the individual awareness levels are not put into focus.

ii. The second limitation of the prototype is that it doesn't consider the organizational structure while coming up with the overall awareness level of the organization. This means that in terms of holding divisional heads accountable on Information Security matters becomes difficult. The regional level is considered a high level of operation. Similarly some people would argue that divisional is still a high level of operation and would opt for departmental.

iii. The lack of input such as Metrics on data that is easily available within the organization such as the number of reported security incidents, percentage of staff who have completed security awareness course etc means that the model is unable to reach high levels of accurate measurement. This is because metrics can contribute significantly at the results used for arriving at possible Information Security awareness levels.

2.6.2 Summary of Kruger and Kearney prototype

The prototype proposed by Kruger and Kearney (2006) provided future researchers with a very good foundation on which to build on in terms of Information Security awareness measurement. Subsequent niche researches were done that built into the prototype in terms of the input required in order for the overall output to be as accurate as possible. The awareness measurement models accuracy and effectiveness is all dependent on the accuracy of the data input. What to measure and how to measure it then has to be considered in greater detail so as to come up with concrete and conclusive end results.

2.6.3 The Veiga, Martins and Eloff Perspective

Veiga, Martins and Eloff suggested that "Organizations need to assess their employees' behavior and attitudes towards the protection of information assets in order to establish whether employee behavior is an asset or a threat to the protection of information." (Veiga, March 2014). Through these organizational assessments on the Information system users, organizations are now in a position to check whether an acceptable level of awareness exists and if the current levels are not satisfactory, the organization is able to decide what action needs to be taken to reverse the levels. They managed to assess the Information security culture using an Information Security Culture Questionnaire. These questions asked in a questionnaire typically looked at security requirements that employees are expected to know i.e. their current knowledge. This argument is supported by an example such as If an employee is not able to recognize an Information Security Incident, then the same employee is not expected to report such an incident.

Security culture can be referred as: How things are done (i.e. accepted behavior and actions) by employees and the organization as a whole, in relation to information security.

Information security culture can be discussed as:

i. A set of information security characteristics that the organization values
ii. The assumption about what is acceptable and what is not in relation to information security
iii. The assumption about what information security behavior is encouraged and what is not,
iv. The way people behave towards information security in the organization

The questionnaire was split into three sections namely:

i. Information Security culture statements - The statements where in a scale the respondents will either agree, disagree in various strengths. The statements generally reflect the attitude of the organization regarding Information Security in the eyes of the respondents.

ii. Knowledge Questions - This section analyzes just how many an organizations' employees are aware of Information Security. The answers required were typically YES /NO answers. An Example of such a question was "I know what an information security incident is."

iii. Biographical Questions - These kinds of questions are important due to their ability to help the researcher differentiate the data and draw comparisons within the population.

2.6.4 The Schlienger and Teufel Perspective

Teufel, Information Security Management, Education and Privacy; through a survey utilized a questionnaire, to gain an understanding of the official rules that influence the security behavior of employees. The questionnaire measured 20 areas; leadership, problem management, communication and attitude. The research according to the authors stated that; “even employees who know their responsibilities in regards with the information security will still disobey information security policies (Teufel, Information Security Management, Education and Privacy, 2003)

2.6.5 The Stanton et. al Perspective

H.A. Kruger presented a paper on the systematical classification of information security end user behaviors that could be used when analyzing security behavior. They stated that due to the intensified need for improved information security, many organizations have established information security awareness programs to ensure that their employees are informed and aware of security risks, thereby protecting themselves and their profitability (H.A. Kruger a, 2006).

They further, stated that in order for a security awareness program to add value to an organization and at the same time make a contribution to the field of information security, it is necessary to have a set of methods to study and measure its effect.

As presented in their findings, their results suggested; "six categories of end user security - related behaviors appeared to fit well on a two-dimensional map where one dimension captured the level of technical knowledge needed to enact the behavior and another dimension captured the intentionality of their behavior. The focus of measurement is on end users behavior with

regards to their intentions and their technical knowhow. They were also able to showcase levels of end user behavior variation in various industries.

2.6.6 The Tessem and Skaraas perspective

According to Tessem and Skaraas, organizations should also consider measuring the level of their in-house information security culture. In this case, the term culture analyses user behaviour in deeper terms than simply, being aware of what is required of a user in terms of Information Security (Tessem, 2005).

They are of the opinion that it is difficult to provide empirical data on information security and it is also difficult to make an accurate analysis of information security awareness. However they propose a few metrics that can be used to establish the level of awareness of staff in a particular organization such as the percentage of an organizations staff who have completed awareness training; the number of reported information security incidents; how many staff member leave confidential Information on their desks and the percentage of lost passwords.

2.6.7 The Mathisen Perspective

Spyros Kokolakis established a set of nine metrics that can be used to measure awareness levels based on interviews he carried out across I.T practitioners drawn from different industries namely financial, telecommunications and manufacturing Industries. (Aggeliki Tsohou, 2004) One of his main observations is that across the industries, the methods used to carry out awareness, approaches used, expected results did not indicate any significant differences. The nine metrics identified by Mathisen that could be used to measure awareness Percentage of employees who have finished the security training.

i. Number of reported Information security incidents
ii. Percentage of employees having a clean desk at the end of the day
iii. Percentage of paper waste shredding
iv. Percentage of illegal traffic on the internal computer network
v. Percentage of weak user passwords
vi. Number of hits to Information security web pages
vii. Number of requests to security department
viii. Customer satisfaction

According to (Aggeliki Tsohou, 2004), the metrics could further be developed into a model that can then be used via a Questionnaire to gain a better insight into how aware an organization's

users are. He further argues that the list is by no means exhaustive and that further metrics could be added to the list of metrics depending on the areas that an organization feels is more important.

2.7 Factors to Consider in establishing an Awareness Measuring Model

2.7.1 The NIST Perspective

According to (National institute of Standards and Technology [NISTL 2009) report, evaluation of Information security training is important. Its importance is due to the fact that it helps the trainer, trainee and organization involved to establish whether their individual and collective needs were met. This roughly translates to measuring of the success of activities that have been engaged in to shore up the levels of awareness in organizations. This is especially important since financial resources and human resources are usually committed into making the project a success. Measurement of activities such as training therefore helps to formulate and utilize effective techniques of increasing awareness levels of Information Security.

According to (NIST, 2009L while considering the effectiveness of Information security training, the following is measured

i. The extent to which right environment for learning and the learner's satisfaction;
ii. Learning outcome and what the student learnt.
iii. Long term pattern of outcomes and what students have been learning over time.
iv. The value of the specific class or training event compared to other options in the context of an agency's overall information security training program; i.e., program effectiveness.

2.7.2 The Kajava and Savola Perspective

Kajava and Savola, (2005) look at factors to consider when coming up with Information Security metrics. They argue that input is required from security objects in order to come up with appropriate metrics when coming up with a model to measure Information Security. A lot of studies have been done that attempt to come up with either a model or framework to measure Information Security in general. Some of the factors that come out as general areas to focus on are such as the pillars of Information Security i.e. Confidentiality, Integrity and availability.

According to (Savola, 2007) they state that measurements offer specific measurable parameters and are represented by numbers, weights or binary statements. In order to avoid confusion, metrics are produced by taking measurements overtime and comparing two or more

measurements with predefined baselines, hence providing a platform for interpretation for the collected data.

(Savola, 2007), stated that techniques of security measurement include risk analysis, certification and measures of Intrusion process. They also argue that Security metrics can be arrived at through the following techniques Goal establishment, prediction, comparison, monitoring and analysis.

2.8 Research Framework

Different innovative models of measuring awareness levels in an organization that have been proposed by different authors were analyzed. Each method had its own unique features and some of them are simple and effective. These studies include among others; Martins and Eloff, 2001, Veiga, March 2014, Teufel, Information Security Management, Education and Privacy, 2003, Tessem, Skaraas, 2005. From the three main factors measured are user behavior, attitude and knowledge possessed in as far as Information Security is concerned. Risk based assessments are used to decide which areas of the business to focus on as far as awareness is concerned.

While attempting to cover as much ground as possible on items considered to be important for respective organizations, simplicity has been the main overriding factor in the creation of the models. Before a measurement model is defined and tested, the key considerations of the business must be identified and must have adequate representation in the model.

Most of the research reviewed, they concentrated on the importance of awareness initiatives and awareness techniques. While some of these research are not necessarily based on a theoretical model, but instead simply provides guidance on what methods to use. However, the researchers admitted that they had no way of measuring the effectiveness of this intervention.

With all these factors having been put into perspective, the prototype proposed by Kruger and Kearney (2006) provided future researchers with a very good foundation on which to build on in terms of Information Security awareness measurement. Subsequent niche researches were done that built into the prototype in terms of the input required in order for the overall output to be as accurate as possible. The awareness measurement models accuracy and effectiveness is all dependent on the accuracy of the data input. What to measure and how to measure it then has to be considered in greater detail so as to come up with concrete and conclusive end results.

3. RESEARCH METHODOLOGY

3.1 Introduction

Effective user security awareness campaign can greatly enhance the information assurance posture of an organization. Information security includes organizational aspects, legal aspects, institutionalization and applications of best practices in addition to security technologies. User awareness represents a significant challenge in the security domain, with the human factor ultimately being the element that is exploited in a variety of attack scenarios. Information security awareness program is a critical component in any organizations strategy. (Khan1 & Alghathbar, 2011).

The general idea of this study was to assess the effectiveness of the automated trading system used by NSE in its information security by measuring the Information Security knowledge possessed by the users of the system. The research aimed at identifying which techniques were used to impart awareness of the security of the system to the users of the ATS. The study was also aimed at designing a model that would be used to measure the information Security awareness levels of users of the system. The model was to be customized in an effort to fit CMAs requirements. This chapter highlights the various methods and procedures adopted in conducting the study in order to answer the research questions raised.

3.2 Research design

A research design is a plan of scientific investigation. This research aims at adopting a sequential two step qualitative research design. The main strategies to be used are a survey and a single case study. This research will tend towards a mixed method format. A mixed methods Research design employs the collection and analyzing of both qualitative and quantitative forms of data in a single study. On one hand it will involve observing and describing the behavior of a subject without influencing it in any way.

3.3 Target population

A population is defined as the total collection of elements about which the researcher wishes to make some inferences. A population element is the subject such as a person, an organization, customer database, or the amount of quantitative data on which the measurement is being taken.

This study aimed at getting from a sample of NSE ATS users at different levels of usage; ATS dealers, ATS network administrators, ATS database administrators, and the general NSE and CDSC employees who interacts with the system.

The research will tried to gather the feelings of the target population on what they think about the user security awareness as is documented in the NSE security policy document. The research also tried to find out whether the user awareness is achieving its objective from the sample population.

3.4 Research instruments

The primary data collection method to be used is questionnaires. Birks, Malhotra singles out reliability, validity and generalization as some of the key advantages of using questionnaires (Birks, 2007). Questionnaires are important data collection tools and they are justified in that they provide an effective and efficient way of gathering information within a very short time. Further, questionnaires facilitate easier coding and analysis of data collected. The questionnaires to be administered included a few open ended questions and also some open ended questions. This is because open ended questions provided an insight of new ideas whereas closed ended questions ensure that the respondents are restricted to certain categories in their responses.

Data collection

Data is a piece of information that helps to analyze and appraise the given problem in a research study. It could be either a primary data, which is collected individually or a secondary data that is obtained from an already existing source.

The data to be used for the research project work is primary data collected from the ATS user respondents, while the data collection instrument to be used will be questionnaires. The questionnaire will have open ended and closed ended questions.

Questionnaires will be sent to a large number of people who interacts with NSE ATS at different levels of usage. We expect these individuals to be more truthful while responding to the questionnaires regarding the system security issues in particular due to the fact that their responses are anonymous.

3.7 Data analysis

After collecting the data, the completed questionnaires were analyzed and screened for completeness, errors and consistency across the respondents. The collected data from the questionnaires were then edited and analyzed using Microsoft Excel. The study was modeled on an exploratory descriptive research.

Descriptive analysis can be described as a process that involves transforming a mass of raw data into tables, charts, with frequency distribution and percentages which are a vital part of making sense of the data (Denscombe, 2001).

4. RESULTS

4.1 Introduction

This chapter presents the findings of the study based on the data collected from the field using questionnaire. The analysis focused on answering the following and establishing of techniques used to impart information systems security awareness and their effectiveness; Establishing of the extent to which NSE organizations measure their information systems security awareness levels; Developing of a Security Awareness Measurement Model that can be adopted in the Nairobi Securities Exchange and testing of the Security Awareness Measurement Model in the Nairobi Securities Exchange and the Capital Market.

A total of 29 individuals responded out of the 40 questionnaires distributed in the five stockbrokers and Investment banks that were randomly selected for the survey.

4.2 Demographic Information

The demographic information for the study comprised of the respondents organization, gender, position in the organization/stock agent, age, educational level, work experience in the organization.

4.2.1 Gender

The research in this section of the research tried to find out the gender of the respondents across the sampled Stockbrokers and Investment Banks under survey. As shown in the fig. 4.0 below, 72% male and 28% female responded to our questions under investigation.

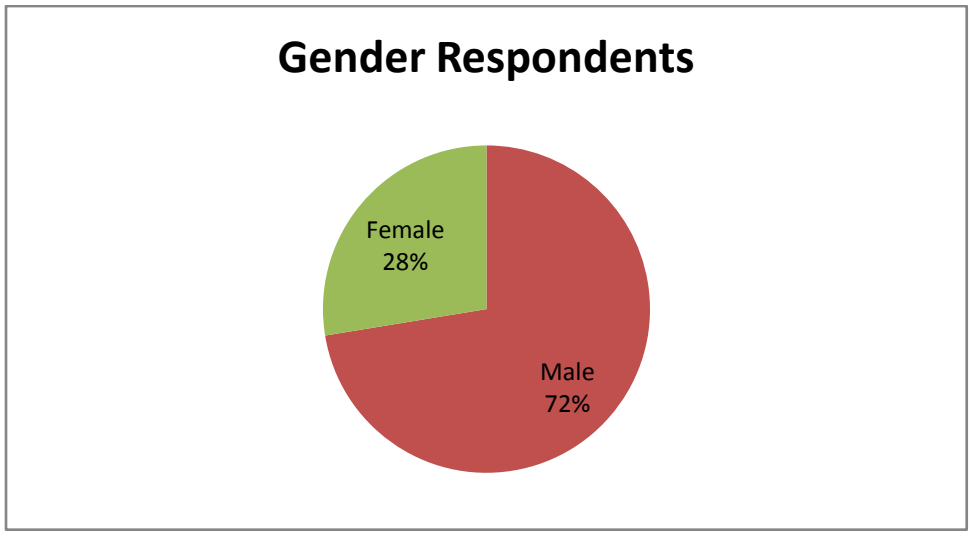


Fig 4.0: Gender of Respondents

4.2.2 Stockbrokers and Investment Banks Surveyed

Out of the 18 stockbrokerage firm and Investment Banks, we randomly selected five firms that were surveyed. Below in the *fig. 4.1* is the distribution of respondents based on the firms.

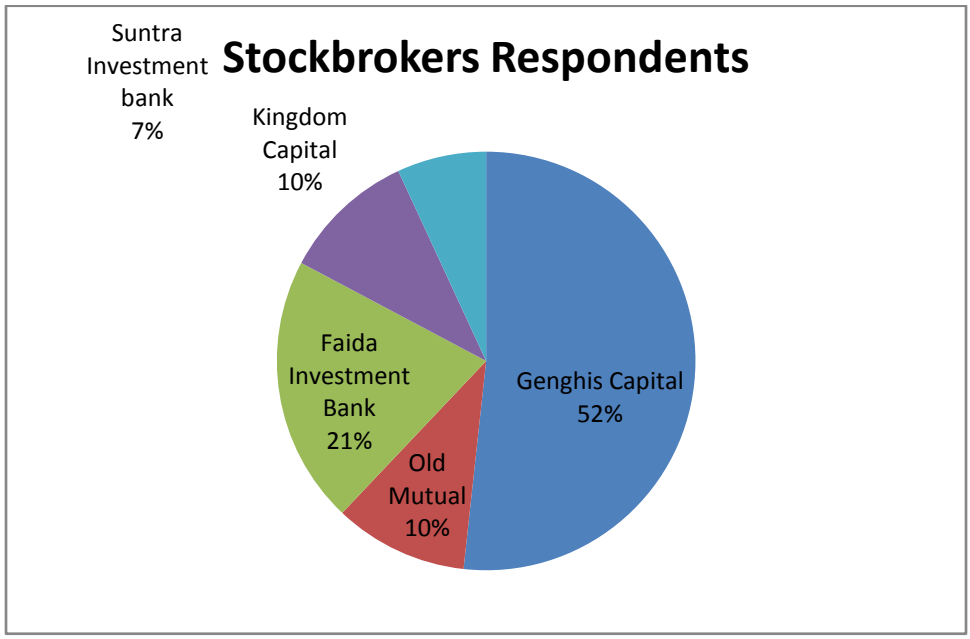


Fig 4.1: Number stockbrokers who responded

4.2.3 Organization structure

In this survey, we see a uniform distribution of all the employees in the various firms surveyed, fall between the ten and one hundred employees. This then qualifies these firms to fall in the category of small and medium enterprises.

We tried to get respondents from across the Stock agents and employees divide. This is critical in that, we have quite a sizeable number of agents who have access to the ATS system at different levels of usage; market viewer module and sell and buy module. Owing to the fact that stocks agents are outsiders, we tried to access whether they have been trained on how to handle the passwords that have been issued to them. This is well represented in *fig. 4.3* below.

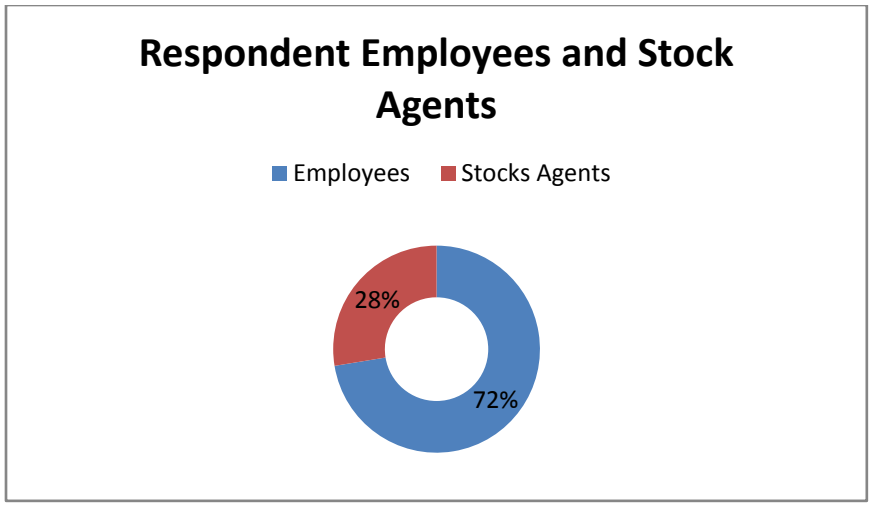


Fig 4.3: Number of Stock Agents and Employees

Out of the 29 respondents, as show below in *fig. 4.4;* forty eight percent are designated as systems end users and twenty eight percent are stock agents. This was a deliberate move since they are one who are more likely to expose the Information security of the company. We also had twenty four percent respondents from the combination of Information systems managers and Information security managers who have been mandate as the custodians of the company information by ensuring that appropriate control s are implemented and maintained in an organization.

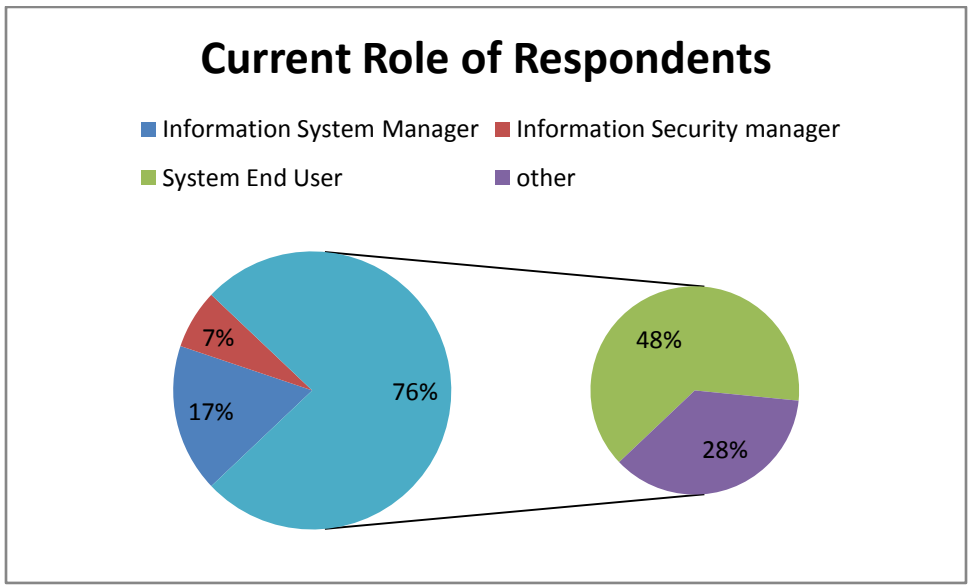


Fig. 4.4: Current role of respondents

As shown in *fig. 4.5* below, the biggest chunk of those who responded have worked for more than five years while those who have worked for the less than a year account for the least number. This can be deduced to indicate a fair level of accuracy in their responses which are based on their observation over the same period of time. The accuracy of the respondents is drawn from their duration in their current position and their direct or indirect role played in Information Security Awareness

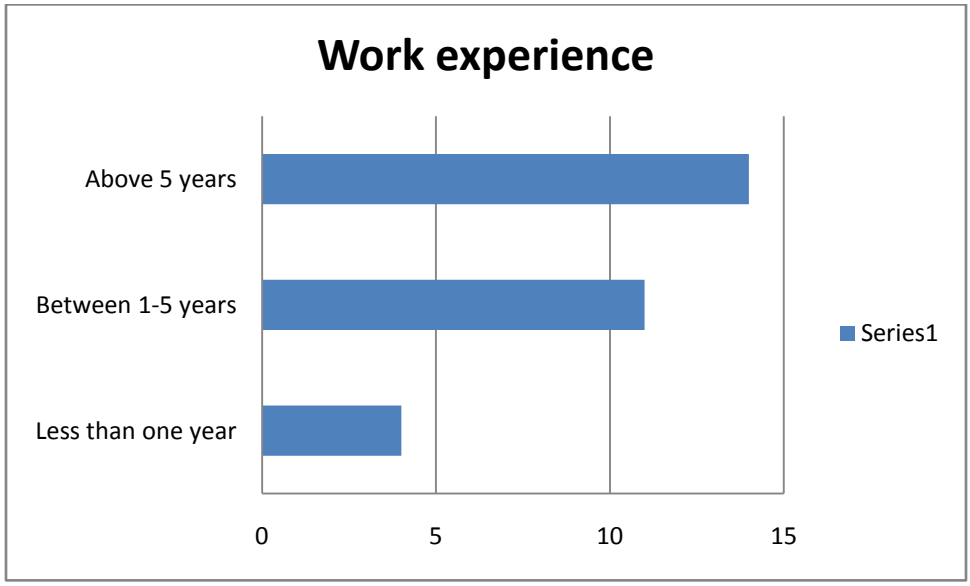


Fig. 4.5: Work Experience

4.3 Information Security Awareness Techniques

4.3.1 *Techniques used to impart Information Security Awareness*

Fig. 4.6 below shows the major Information Security Techniques and the responses received in terms of usage.

The results also shows that the Information Security Awareness techniques which had the lowest usage among the respondents were lack of information security awareness induction courses and lack of proper information security awareness trainings. Across all board, all respondents gave a negative response on these two; "When you were employed/given stockbrokerage agency, were you taken through the Information security awareness program as part of your induction?" and "Is the information security awareness training mandatory? ". The researcher in the literature review had identified that most organizations do not have different content targeting different

members of the organization e.g. senior management content as compared to that of junior staff content. However the existence of the different content would then make it more complex to measure an organizations' Information Security awareness.

From the researchers understanding, lack of proper understanding of the importance of Information Security awareness from the persons mandated with the training and dissemination of information security information, hence their lack of inclusion in the normal mainstream organization training on Information Security awareness courses.

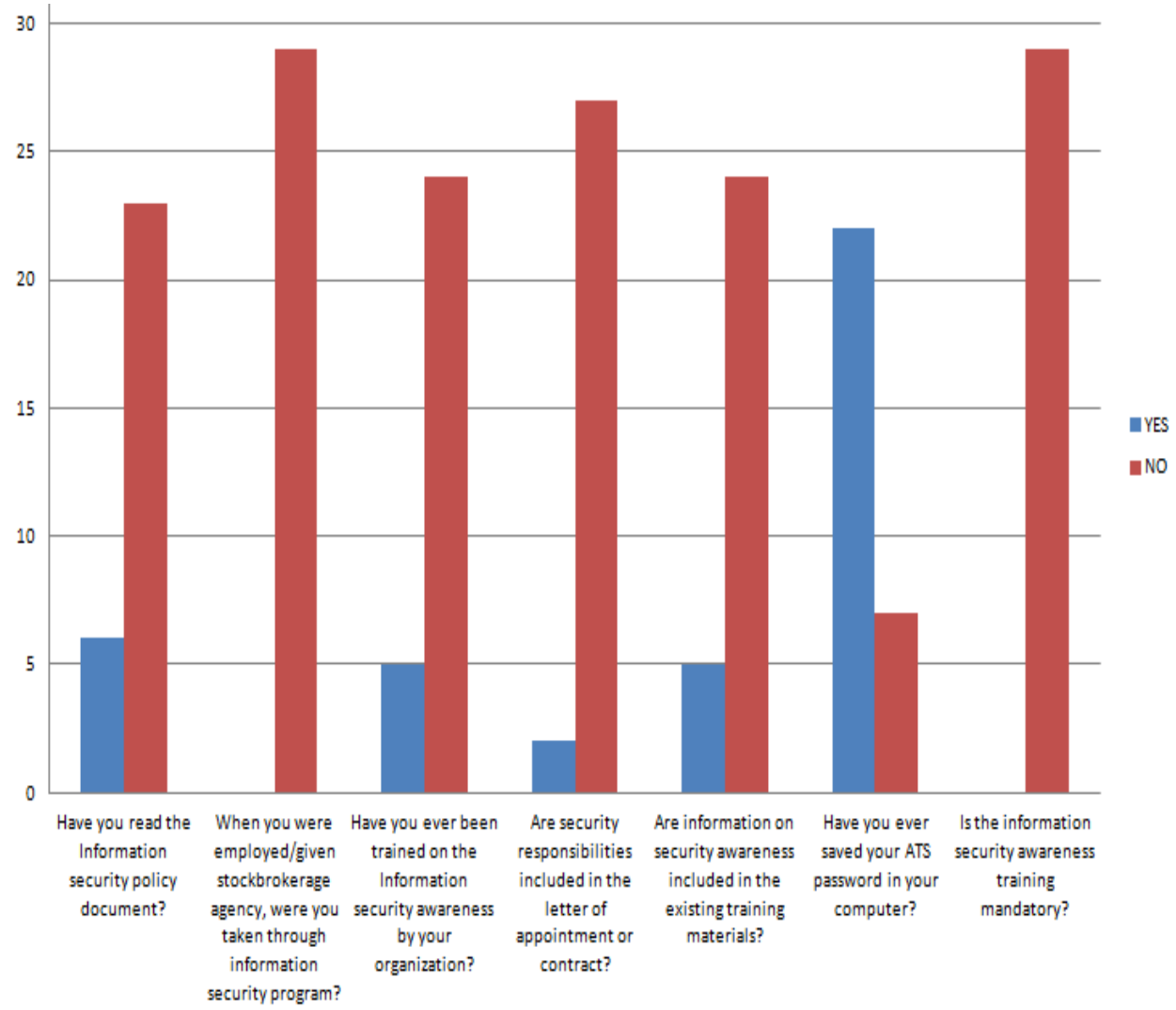


Fig. 4.6: Techniques used to impart Information Security Awareness

4.3.2 *Information Security Awareness Techniques Effectiveness*

Fig 4.7 is a snapshot of the responses given indicating the effectiveness of the Information Security techniques that are used to spread Information Security awareness in the various NSE organizations that were surveyed.

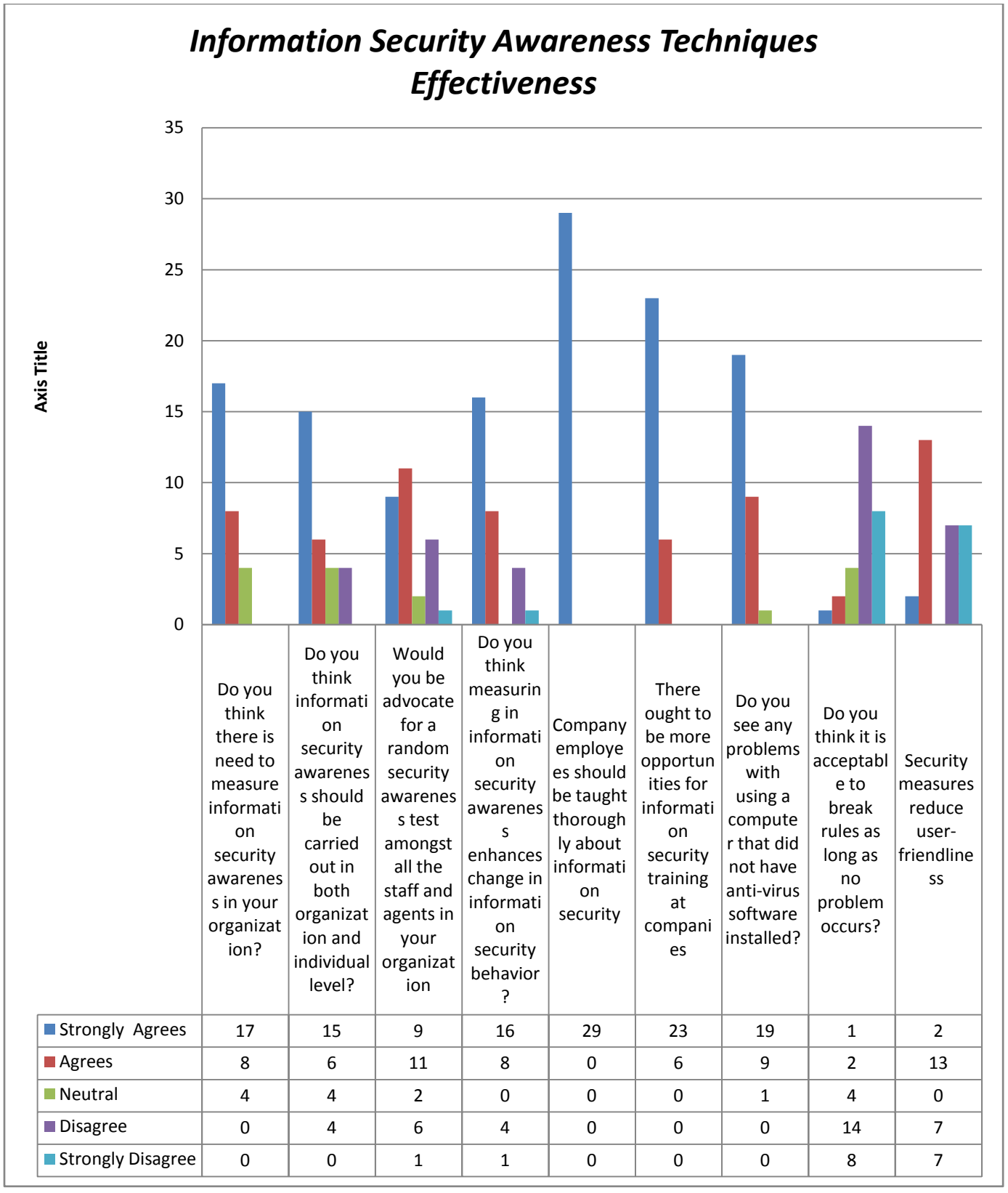
The findings from the figure 4.7 are presented in the format of 'Strongly disagree' being the least effective while 'Strongly agree' being the most effective progressing from bottom to top, this is in the exception of the question; "Do you see any problems with using a computer that did not have anti-virus software installed?" and "Do you think it is acceptable to break rules as long as no problem occurs?" whereby, we expected a negative response.

Company employees should be taught thoroughly about information security in-house and on a continuous base, was selected by the highest number of respondents compared to the other techniques as the most effective technique to spread information Security awareness in an organization.

The other favourable technique by number of respondents is that; there ought to be more opportunities for information security training at companies. This further underscores the need for a thorough and continuous training at all levels possible to disseminate the security information to the employees.

The results indicate that in terms of effectiveness, all other Information Security Techniques were considered as generally effective in a scale of 1-5 from least desirable to most desirable i.e. Most of the respondents selected between 3 to 4 indicating that in general most respondents did not select 1 and 2 which were representing their opinion in terms of least effectiveness of their Information Security techniques.

Other opinions offered by the respondents indicate that by measuring Information Security Awareness in the organization it would greatly enhance change in information security behaviour.



	Do you think there is need to measure information security awareness in your organization?	Do you think information security awareness should be carried out in both organization and individual level?	Would you be advocate for a random security awareness test amongst all the staff and agents in your organization	Do you think measuring in information security awareness enhances change in information security behavior?	Company employees should be taught thoroughly about information security	There ought to be more opportunities for information security training at companies	Do you see any problems with using a computer that did not have anti-virus software installed?	Do you think it is acceptable to break rules as long as no problem occurs?	Security measures reduce user-friendliness
Strongly Agrees	17	15	9	16	29	23	19	1	2
Agrees	8	6	11	8	0	6	9	2	13
Neutral	4	4	2	0	0	0	1	4	0
Disagree	0	4	6	4	0	0	0	14	7
Strongly Disagree	0	0	1	1	0	0	0	8	7

FIG. 4.7: INFORMATION SECURITY AWARENESS TECHNIQUES EFFECTIVENESS

4.3.3 Problem affecting Information Awareness in the Organizations

The Fig 4.8 is clearly illustrates that lack of information awareness content is one of the main reason that they don't have any training on information security awareness. 'Lack of time', ranks as the second biggest problem, negatively impacting information security awareness in these organizations.

Information security awareness not being a priority across all the organizations is cited as the least reason negatively impacting the carrying out of Information Security awareness. According to the responses, lack of resources at the organizations is not a major negative factor, however the same reason has manifested itself in other forms such as Individuals in organizations not taking Information Security with the seriousness it deserves.

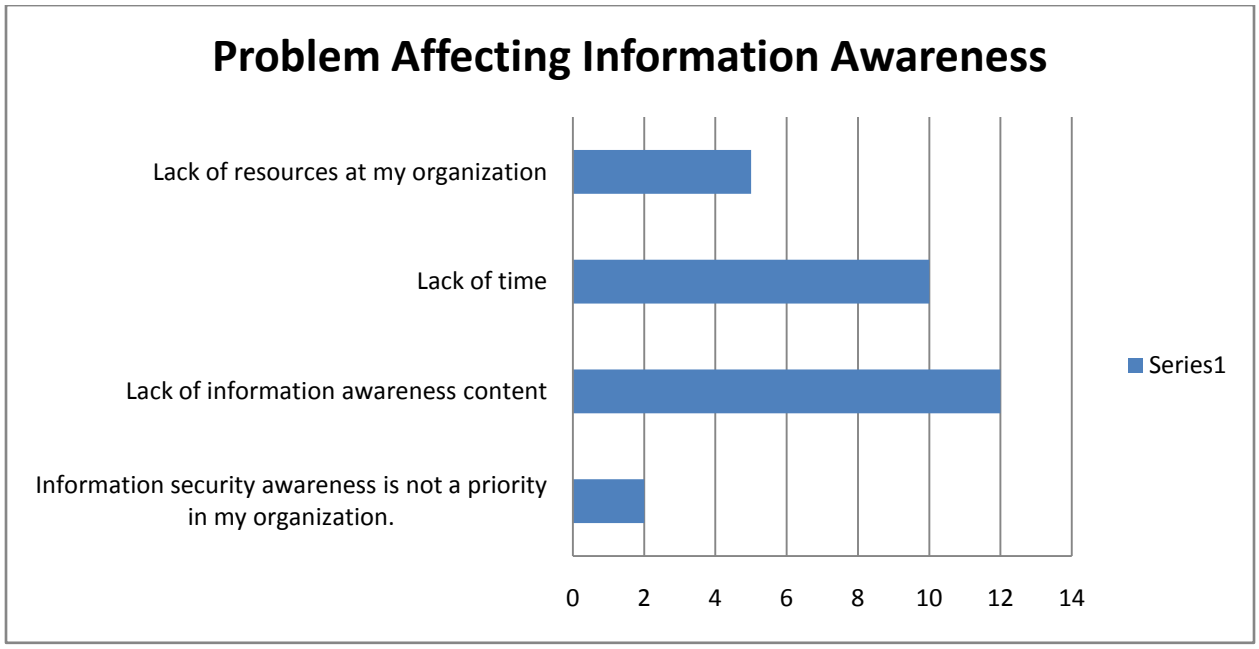


FIG. 4.8: PROBLEM AFFECTING INFORMATION AWARENESS

4.3.4 Outsourcing of Information Security Awareness

As illustrated in *fig. 4.9 below*, an overwhelming sixty six percent of the respondents would gladly welcome outsourced services of Information security awareness while only thirty one percent are opposed to a move of that nature of fully outsource Information Security awareness. Interestingly, only three percent are not sure whether to outsource or not.

From these responses, there is a perceived interest in outsourcing Information Security considering the reasons cited for not conducting Information Security awareness such as

Information security awareness is not a priority in my organization and lack of time. Lack of time would normally affect even the recipients of such training. However the support of Management would actually enable creation of time and content to facilitate the awareness training since there is a general lack of acceptance to outsourcing of the awareness training.

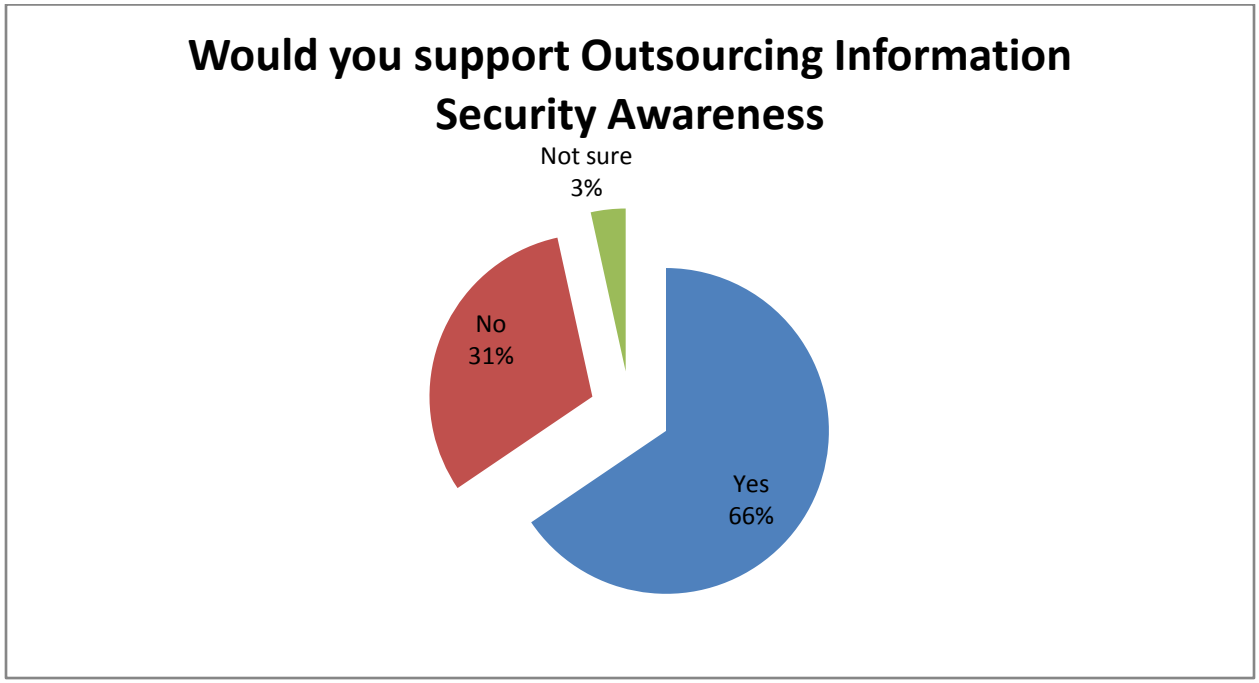


Fig. 4.9: Outsourcing of Information Security Awareness

4.4 Measurement of Information Security Awareness levels Findings

The findings regarding Information Security Awareness measurement will feature in the eventual model that will be proposed by the researcher. The respondents will have therefore provided information in to aspects of the model that they would like included. This research was focusing on the sampled Nairobi Securities Exchange brokerage firms and Investment banks, hence this model might not work very well for other sectors but might be adopted in other countries on their stock exchange.

4.4.1 Need to Measure Information Security Awareness

From the findings as shown on figure 4.10, there is strongly resounding agreement from almost all the respondents that there is a need to measure. Only two respondents who did not think there is need are neutral on whether to measure security awareness.

This therefore means that if provided with an adequate model that they can use, the respondents would utilize that model to gain visibility into their organizations staff levels of awareness. Armed with that knowledge, they would then chart away forward to address any concerns raised.

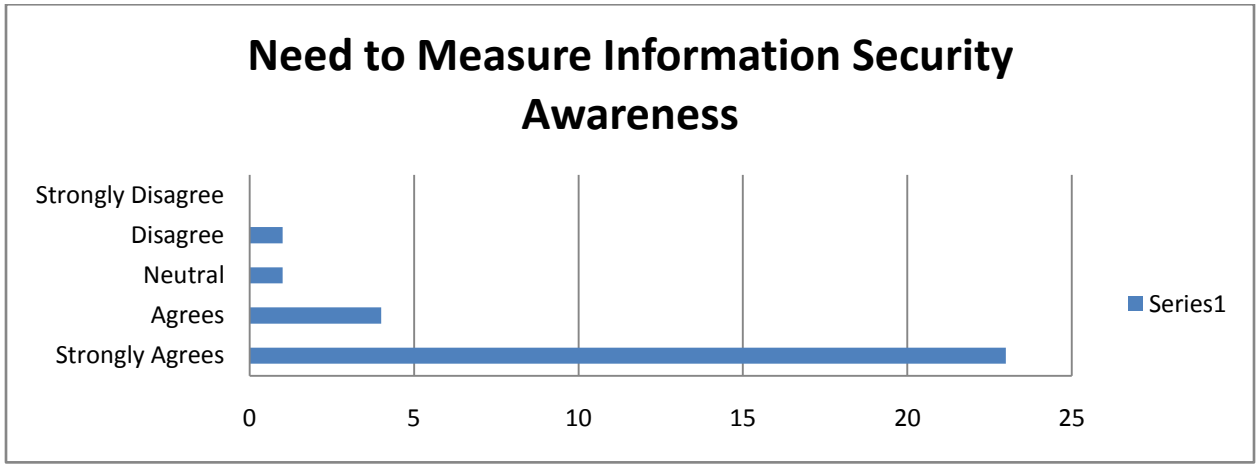


Fig. 4.10: Need to measure information Security Awareness

4.4.2 Measuring of Information Security Awareness Levels enables an organization measure change in behaviour

The findings in Figure 4.11 indicate that most respondents agree with the fact that measurement of awareness levels would assist them in establishing whether there is any change in behaviour in their staff as a result of the knowing their awareness levels.

This can be explained in that once gaps are identified in an organization Staff on their level of awareness; they will endeavour to correct the gaps such that in the next subsequent measurement, they will perform better. This will be manifested in their application of their knowledge as well.

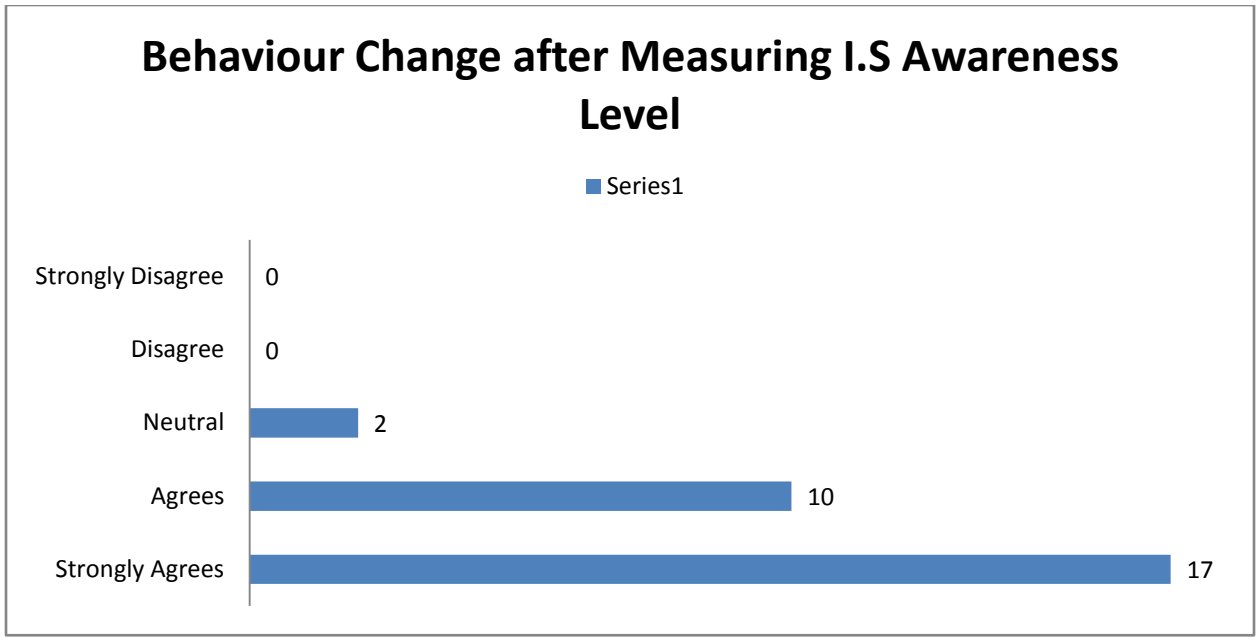


Fig 4.11: Behavior Change after Measuring I.S Awareness Level

4.4.3 Information Security Awareness Measured at Individual and organization level

Figure 4.12 indicates that majority of the respondents would prefer to measure awareness levels both at individual levels and organization levels. Only one respondent disagreed with the need to measure awareness at individual and national levels.

This will assist the organization to be able to chart the way forward in their Information Security strategy. The organization will also be able to assess its individual staff in a bid to ensure that they meet the required knowledge and attitude standards that the organization has set out.

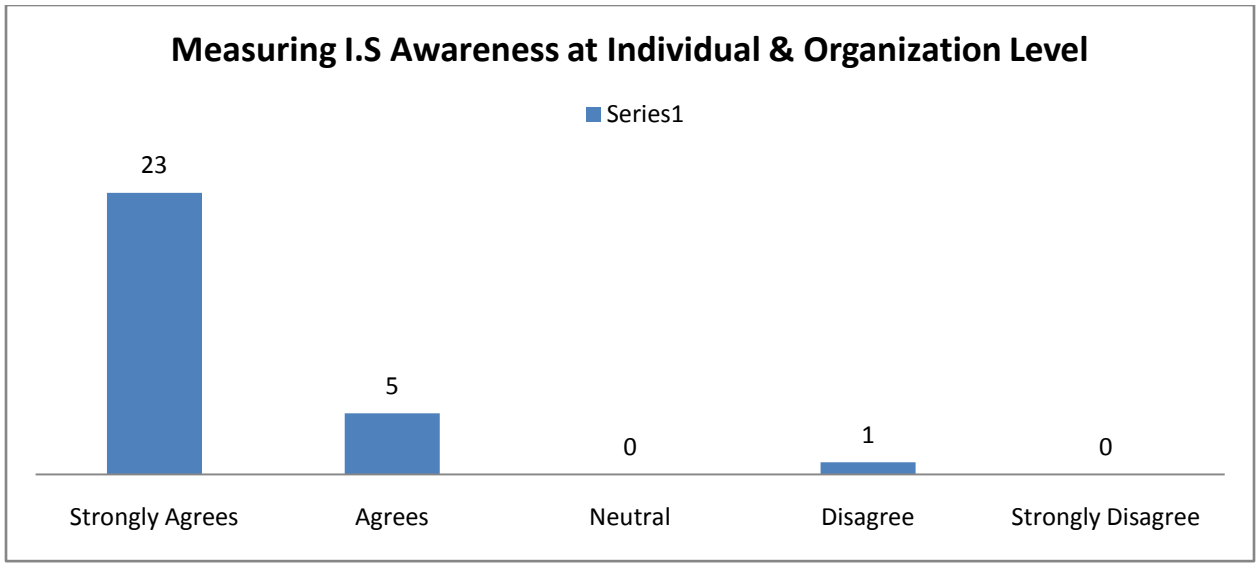


Fig. 4.12: Measuring I.S Awareness at Individual & Organization Level

4.4.4 *Vocabulary test to Measure Awareness levels*

A Vocabulary test of Information Security Terms is a model proposed by (Steyn, 2010) as a means of measuring Information Security awareness in an organization. We have the respondents of an example of a Vocabulary test to put them as below.

Example 1: Vocabulary test

Phishing is:

(a) ☐ *The use of an email message, that appears to be legitimate, to solicit personal details*

(b) ☐ *Part of social engineering which means that someone is persuaded to give away confidential information.*

(c) ☐ *Also referred to as identity theft.*

(d) ☐ *All of the above.*

(e) ☐ *I don't know what the term phishing means*

From the feedback received from our respondents, majority took a 'Strongly disagree' position and generally the overall response seemed to flow towards disagreeing with the view of taking a vocabulary test.

Figure 4.13 is an indicator of the respondent's opinion of how they consider vocabulary testing as an effective method of measuring awareness levels. There was a general disagreement with the idea of simply suing vocabulary to test awareness since most were either strongly disagreed and disagree with the whole notion.

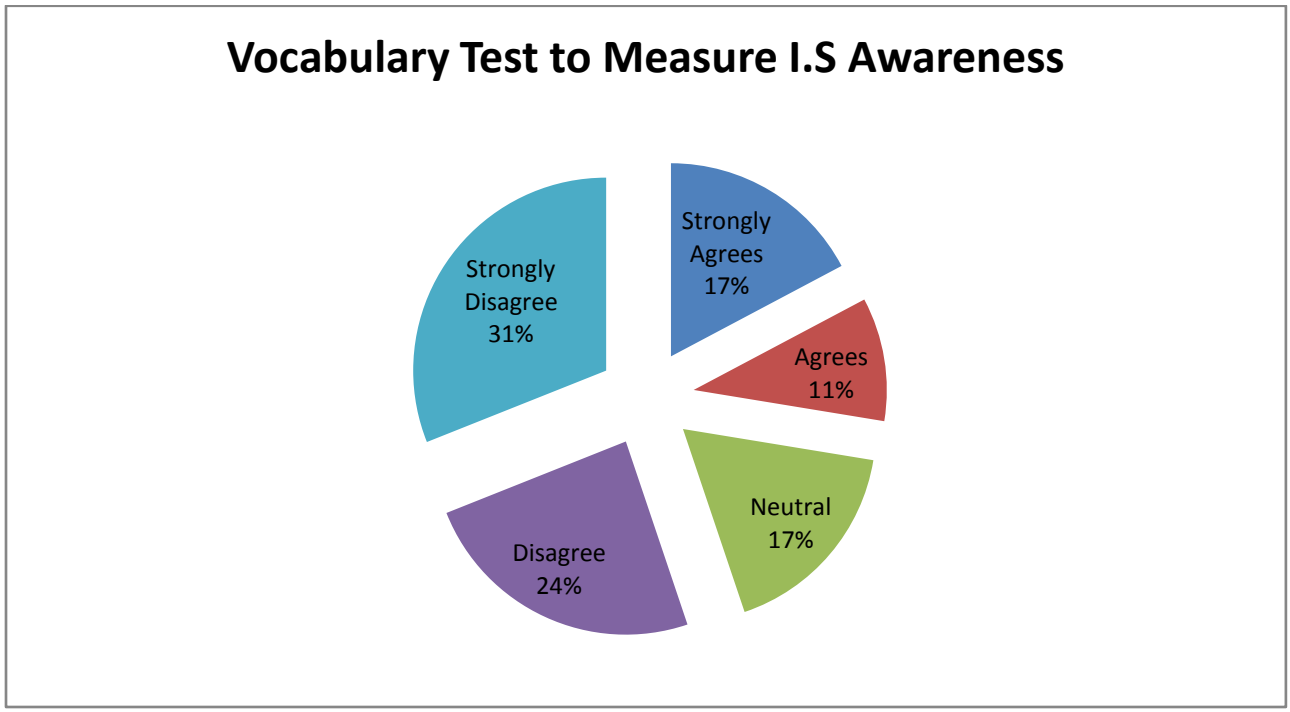


Fig. 4.13: Vocabulary Test to Measure I.S Awareness

4.4.5 Scope of Measuring Information Security Awareness levels

The findings in figure 4.14 indicate the respondent's opinion on the scope with which the measuring of Information Security awareness levels should cover. An overwhelming 83% of respondents are of the favour of covering all levels of Information Security Awareness where information is involved. Only a merger 17% of respondents were of the view that only the critical areas should be covered.

While this approach may have good intentions, it may also turn out to be practically difficult to implement due to the factors such as lack of time which was cited as the reasons that deter Information Security professionals from carrying out effective Information Security awareness. The awareness Measurement model will therefore take a more practical approach that will include the measuring of critical information Security items with priority.

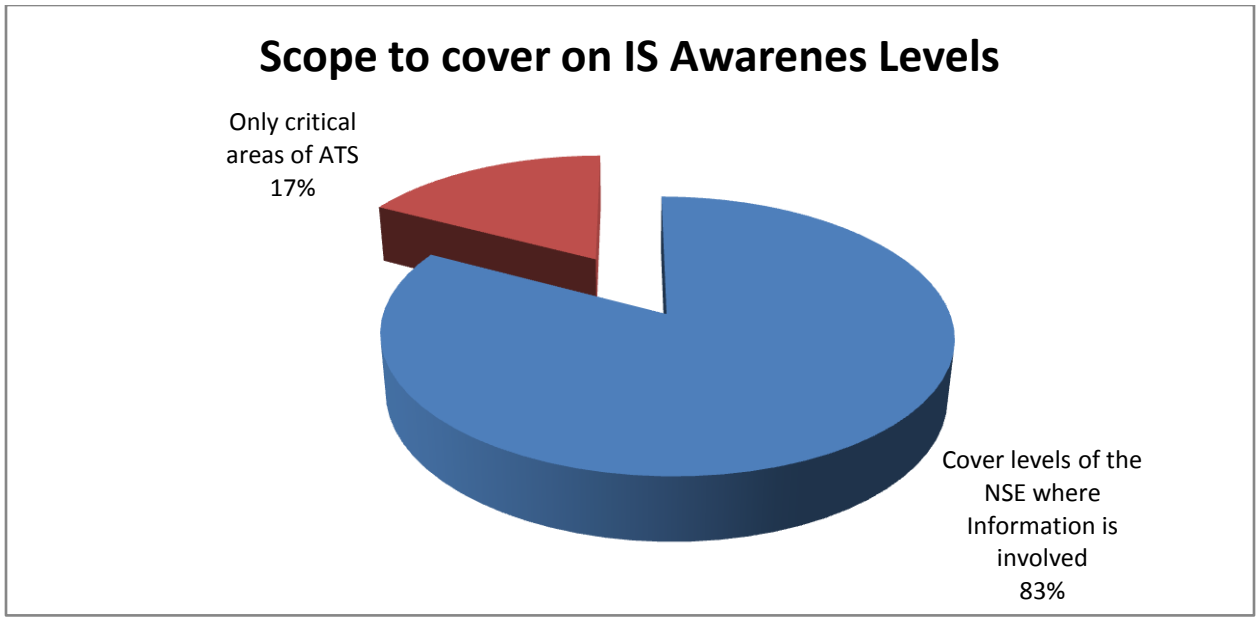


Fig. 4.14: Scope to cover on IS Awareness Levels

4.4.6 Levels of Awareness Desired by Respondents

The analysis found in figure 4.15 of the results above indicate that fifty percent of the respondents would prefer to have a staff population that has internalized Information Security knowledge. Thirty one percent of the same population would settle for a general acceptance of Information Security practices if the first option was not available to them.

The general opinion by the respondents indicates that most of them would prefer a staff population that is aware of Information Security risks and has internalized them in their day to day operations as opposed to mere knowledge which has not been accompanied by lack of willingness to practice it. This can therefore mean that the aspect of measuring of levels awareness will be done with the expectations that it will help improve awareness levels within an organization.

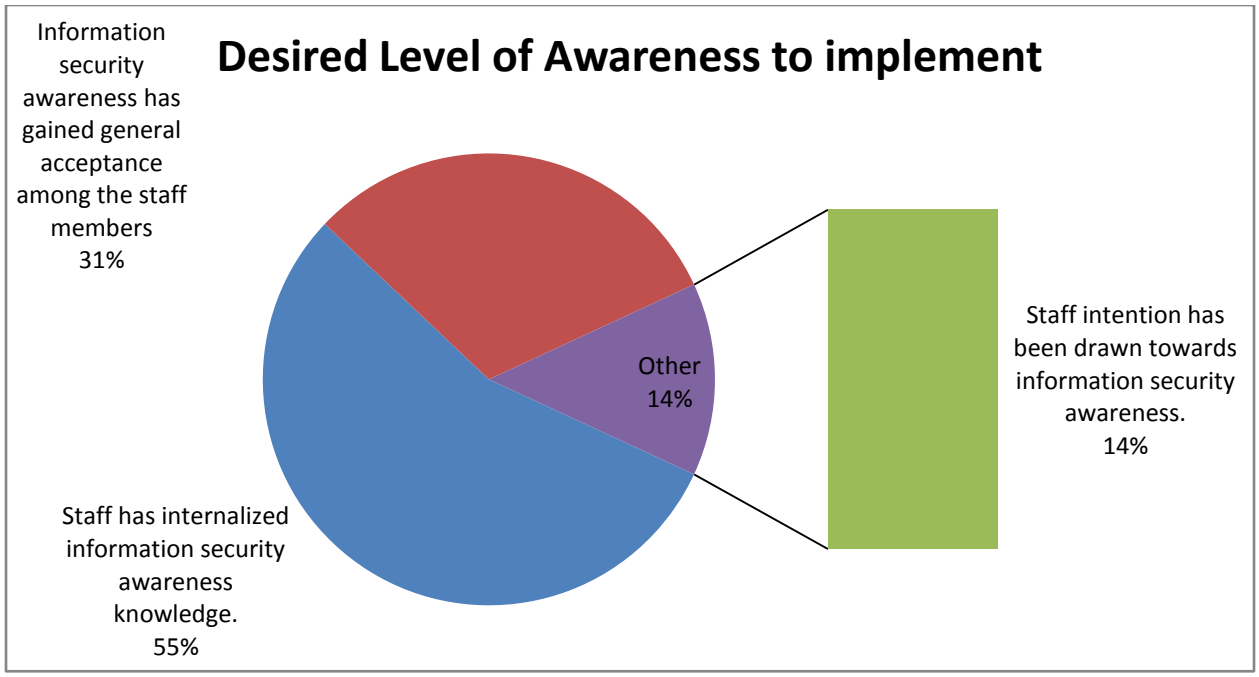


Fig 4.15: Desired level of awareness to implement

4.4.7 Information Security Awareness Metrics

The findings in figure 4.16 indicate that out of all the respondents, only three metrics were selected by over fifteen percent of the respondents. Percentage of weak passwords ranked first at thirty five percent and number of hits to the information security webpage coming at a distance twenty four percent and number of request to security department coming in at number three with seventeen percent. We note that 'Percentage of employees having a clean desk at the end of the day' didn't get a single nod.

The Metrics that are easily available in form of statistics within the organization proved to be popular as a source of information to measure awareness levels. The metrics will also be considered as input into the design of the Information Security model.

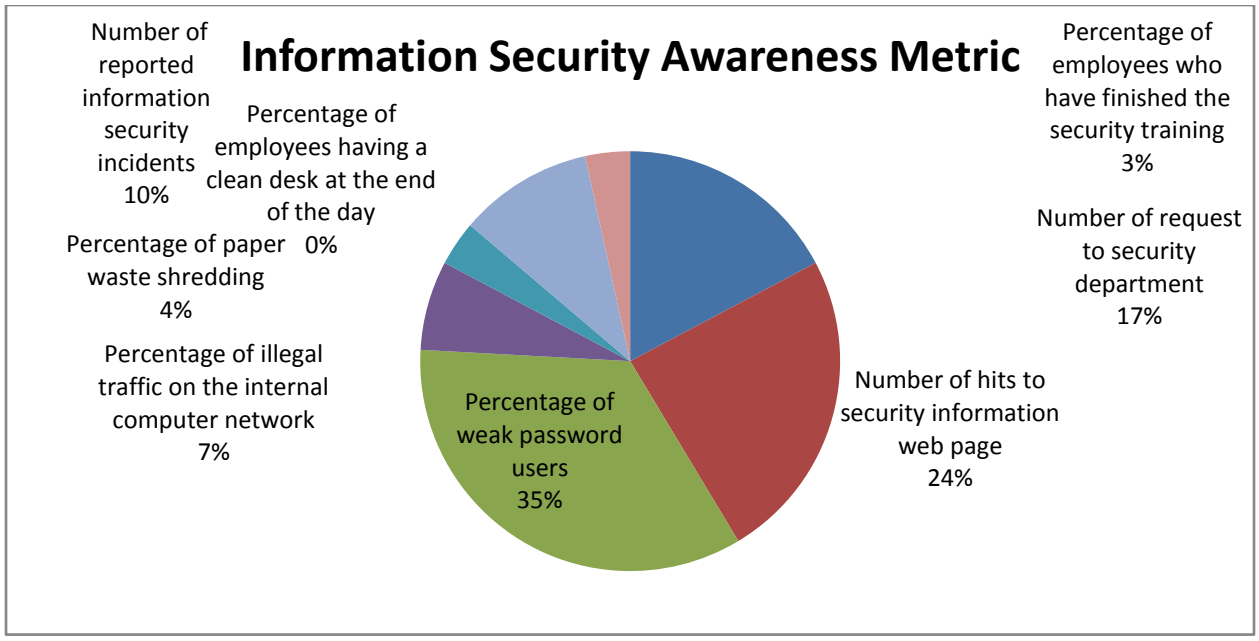


Fig 4.16: Information Security Awareness Metric

4.4.8 Structure based Measurement

The findings in figure 4.17 indicate that the respondents overwhelmingly preferred measuring awareness levels at different organizational structure levels. Seventy nine percent of the respondents selected that awareness levels should be categorized in the three measures of choice. The regional approach was selected by the least number of respondents. This is an indication that it may not truly reflect the true position of an organization in terms of awareness levels since different regions face varying risks.

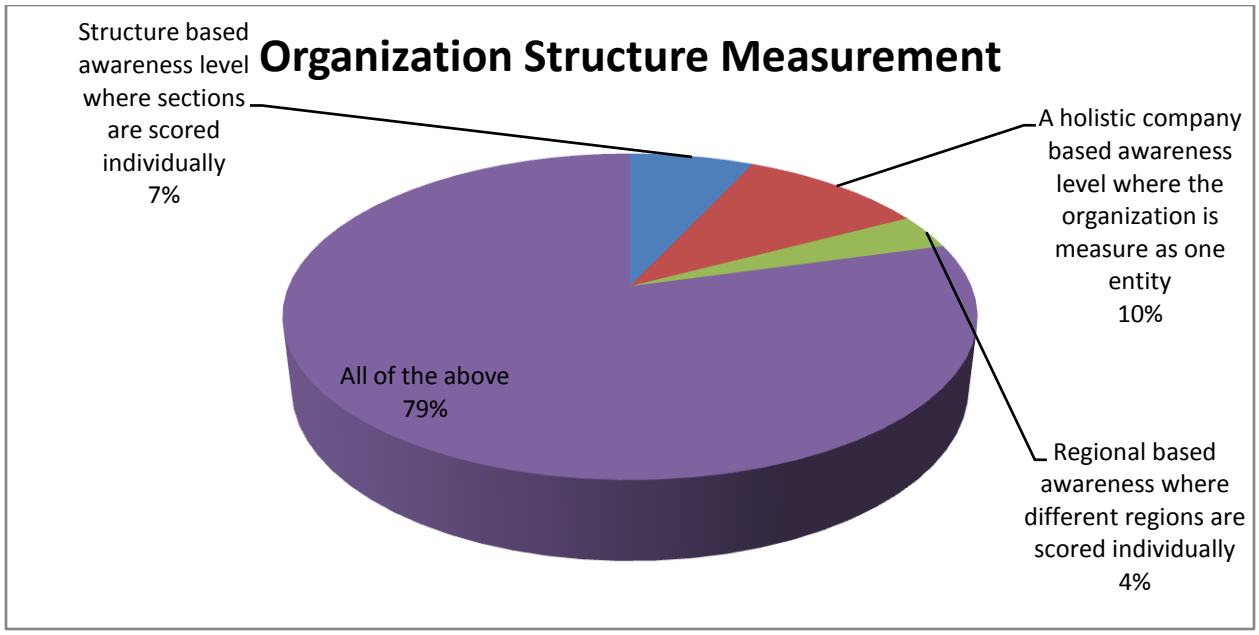


Fig. 4.17: Organization Structure Measurement

4.5 Conclusion

The results in this chapter were in two sections. The first section was looking at the various techniques used to impart awareness and their effectiveness. The second section was building on various models used to measure awareness levels in organizations and seeking the input of the industry professionals. With these results from this chapter, they will come in handy during the formulation an information security awareness model that can be used across the various stock exchanged around the World.

Analysis of the awareness techniques indicated that most organizations are already conducting awareness initiatives at various levels and capacities. It also showed that most of the same organizations are facing challenges both in terms of carrying out awareness activities and measuring awareness levels. This research is focusing on the measuring of awareness levels.

Following the analysis of the responses received, the results indicate that a model to measure awareness levels in the Nairobi Security Exchange is necessary since there is a need to measure awareness levels. The model will also incorporate the input from the analysis in so as to make it more feasible and practical to implement in any organization.

5. PROPOSED SECURITY AWARENESS MEASUREMENT MODEL

5.1 Introduction

This chapter explores the proposed Information security awareness measurement model based on the findings from the previous chapter and also based on the existing security awareness measurement model in other previous works from other researchers.

Measuring Security Information awareness poses two distinctive challenges; what to measure and how to measure it. Requirements such as sustainability ease of use, the use of scientific methods and complying with the organisation's unique requirements, all adds to the challenge of finding a suitable methodology to create the measuring tool with. It is hence prudent to decide to measure the three dimensions; knowledge *(what you know)*, attitude *(what you think)* and behaviour *(what you do).*

5.2 Features of the proposed Model

Based on the empirical study of the various earlier study on Information Security Awareness frameworks and model, the proposed model will be an improved version of the Kruger and Kearney model. A detailed explanation on all the changes that will be effected to the current model will be availed later on in this chapter. The changes are considered as improvements to the model in an effort to align it to the stock market industry. This is so since this research is purely done on the Nairobi Securities Exchange and its affiliates.

From fig. 4.20, the researcher has Regions A and B representing other regions that the organizations may want to measure their awareness levels. This will eventually contribute to the aggregate performance of the awareness levels of a particular region. In the Division section, it is important to note that A and B represent other divisions that an organization would have and that they would assume the same lower hierarchy that Division C has as demonstrated in figure 4.20. In the same regard, the hierarchy that applies to staff B, will be the same that will apply to Staff A and B were it to be populated.

Figure 4.20 contains sections that appear with a dotted line. Those sections represent the modifications and additions included so as to enable the researcher propose a model. The changes were introduced as a result of the analysis of the feedback from the respondents.

In this model, the question of what to measure and how to measure is captured in four main areas. The areas were decided on based on the responses received in the survey. The main areas (dimensions) of awareness to be measured were included in the model as follows:

a. Knowledge - The knowledge that general staff have concerning Information Security with respect to the organization in which they work for is very important. The knowledge that the organizations' staff have can enable the individual carrying out the process to measure awareness is able to c1assify individuals, divisional teams, regional teams and the organization as a whole in terms of the general levels of awareness. An example of one way of c1assification is as proposed by (Teufel, A Conceptual Model to Understand Information Security, 2003) they can be easily classified as "become aware" to "stay aware" and ends up in "be aware". This dimension will also be broken down into five factors of Information Security as indicated in figure 4.20. The knowledge is normally passed to them via the Information Security awareness Techniques discussed in chapter four. In this dimension the following five main focus areas will be utilized to feed into the model:

   i. Password management
   ii. Email Management
   iii. Internet and Social Media
   iv. Social Engineering ***(****the art of manipulating people so they give up confidential information.)*
   v. I.T Security Policy

b. Attitude - The attitude refers to the perception that employees have towards Information Security in the organization. It is normally looked at separately from the knowledge that the organizations' staff have. The reason is that the Staff maybe aware of the rules and regulations concerning Information Security but may not be willing to implement them. The five dimensions that are broad in nature will be broken down into smaller factors that are easily measureable.

   The main focus areas that will be considered in this step are the same the factors in the first dimension i.e. Password management, Email Management, Internet and Social Media, Social Engineering and I.T Security Policy.

c. Metrics - The metrics are easily available information within respective organizations. This Metrics provide a more accurate source of input data in as far as Information Security awareness is concerned. They are also a great indicator of the changing behaviours of the organizations' staff in as far Information Security awareness is

concerned. The main metrics that will come in directly to the model as input are as follows:

i. Number of reported Security Incidents
ii. Percentage of completed Security training
iii. Percentage of Weak user passwords
iv. Number of Requests to Security department
v. Number of hits on Information Security web pages

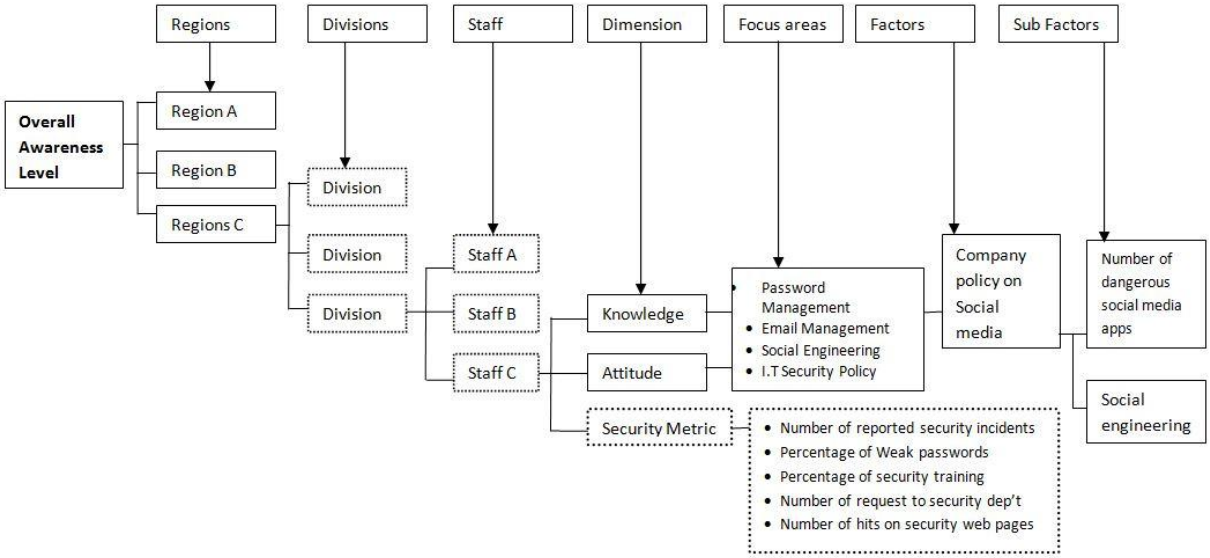


Fig 4.20: Proposed Information Security Awareness Measuring Model

5.2.1 Modifications and Additions to Proposed Model

The model proposed by the researcher as shown in Figure 4.20 was modified in an effort to customize it to local requirements. The additions and modifications to the model were as detailed below.

a. **Individual awareness level (Staff)** - This level was introduced in the model so as to give the Researchers and intended end user of the measurement tool visibility into individual performance of all the organizations users. According to some of the respondents, in some organizations it is mandatory to undertake the Information Security awareness course hence it is necessary for the same individuals to have individual scores. From observation, in highly Security conscious organizations, the pass mark of the Individuals

is normally factored in to their annual performance appraisal at the end of the year. This is done to ensure that the organizations' staffs take Information Security seriously.

b. **Divisional level** - This represents the lowest group based score accommodated within the model. In this case, the researcher proposes to have all structural teams i.e. in most organizations they are known as divisions separated so that the cumulative score of all individuals becomes representative of the division. This was implemented as a result of most respondents requiring a model that will show the performance of the respective divisions in terms of Information security. In some organizations, overall division score may be factored in to the annual performance score for each division.

c. **Regional Level** - This level represents the biggest grouping under the overall awareness of an organization. This model was built with organizations such as Equity Investment Bank Ltd in mind which have regional presence. Some of the respondents who work in similar organizations and would therefore like to have regional representation in terms of awareness levels within an organization. The need to measure organizations in terms of regions is also due to the weightings whereby one region may be allocated more weighting than another due go sub factors such as number of staff, levels of risk and general exposure to computing and Technology.

d. **Additional Metrics levels** - The additional Metrics added represent an accurate source of input data into the model that will assist to give the model a different source of information that is based on statistics easily available in the organization. This is also an addition to the model to make more it all round as an effective Information Security awareness measurement tool, the statistics are collected independently of the other information.

   The proposed Model works through two sources of data input. The first source of data collected is in the form of surveys that the organization will administer to all users. Their responses are then fed into the model which then calculates using a formula similar to the scorecard formula so as to propagate the input values to eventually end up with an overall score for the organization. This will also end up providing, individual, divisional and regional scores as well.

5.3 Validation of proposed Information Security Awareness Measurement Model

The model as explained in the previous section requires two different sets of data input. The first type of data input is from a survey type of questionnaire that is fed provided to all staff or a sample of the organization population. The feedback is then entered into the model. The second source of data input is from selected metrics as per the organizations determination.

i. The researcher proposes to validate the model by utilizing the following steps:
ii. Select on linear section of the model
iii. Allocate Weights to each section of the model
iv. Enter data into the model for each region
v. Present results.

The four steps above will help allow the researcher to validate the model and how it works. Any issues identified will also be addressed accordingly in order to make the model practical.

5.3.1 Simplified Section of the Model

This simplified section of the model represents a broken down simplified version of the model. The model flows from the source of data input through to individual scoring, divisional scoring, regional scoring and finally to overall awareness score of the organization. The simplified model will be used to illustrate how the model is intended to work.

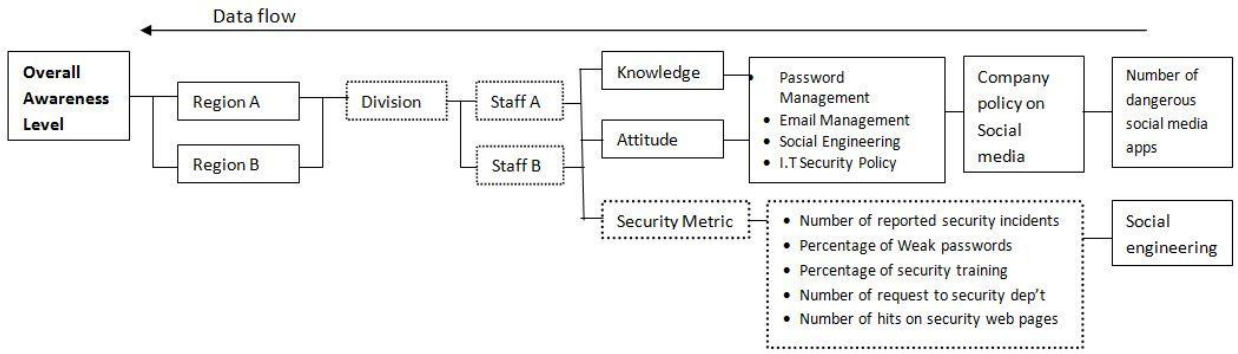


Fig 4.21: Simplified Information Security Awareness Measuring Model

In this simplified model, input will be received from two members of staff. Data input will also be received in the metrics side in terms of the percentage of completion on Information Security awareness courses.

The simplified model as shown in figure 4.21 will be the base of the validation exercise. The model has one division and two regions for purposes of comparison and allocation of weights. The three dimensions will remain intact in the model. However the focus areas have been reduced to two areas namely Internet and Social Media on the user response based section and percentage of completed Information Security awareness training on the Security Metrics dimension.

The factors under the internet and social Media focus area will be the Social Media Policy and sub factors will be Dangerous Social Media Applications and Social Engineering.

5.3.2 Allocation of Weights to different Sections of the Model

Allocation of weights will be done at two section s of the simplified Model. The first section is on the dimensions area whereby the different dimensions will be allocated different weightings. The weights will be determined based on the Researchers own best knowledge on analysis of Genghis Capital requirements.

The second section where the weights will be allocated is the Regions stage. Based on the researcher's observation, different regions carry different weights in terms of Information Security due to reasons such as computing knowledge and exposure from region to region.

In this simplified Model, the weightings will be determined in terms of percentages. As indicated in the table below:

Level	**Type**	**Weighting**	**Representative**
Region	Nairobi	60%	0.6
	Central Kenya	40%	0.4
Dimensions	Knowledge	50%	0.5
	Attitude	30%	0.3
	Security Metrics	20%	0.2

Table 1.2: Table of weightings

The model has been designed to be flexible in terms of weights allocated. The weights are determined by the management of respective organizations based on what the organizations. The weights are then applied to the raw data and together the new data is able to formulate an overall organizational awareness level as well.

5.4 Validation Summary and Conclusions

The model was validated through an MS Excel worksheet. This was the most ideal software to handle this due to its ease of use in terms of test data analysis and manipulation. The Excel worksheet took on the form of the simplified model in an effort to take the same data flow as the model. The flow of data is processed as follows until overall awareness levels are identified:

i. Raw data is entered into the excel sheet
ii. The raw data is computed into totals for each individual. Individual Scores are noted
iii. The individual performance data is weighted out of 100%
iv. Individual scores are aggregated to form divisional scores
v. Divisional Scores are aggregated into regional Scores
vi. Regional scores are weighted as per the weights selected by the management.
vii. Weighted Regional Scores are aggregated into final Organization scores

The following 'IF' formula was used for the validation purposes.

=IF(H392>80,"5 - Excelent",IF(H392>70,"4 - Very Good",IF(H392>60,"3 - Good",IF(H392>50,"2 - Pass","1 - Fail"))))

Region	Staff	Knowledge	Attitude	Metrics	Individual Score (%)	Division Average Score	Overall Organization Score	Overall Organization Rating
Nairobi	Staff 1	64	69	60	**64.33**			
	Staff 2	74	57	45	**58.67**	61.50		
Central Kenya	Staff 1	70	65	62	**65.67**		57.67	2 - Pass
	Staff 2	34	57	35	**42.00**	53.83		

Table 1.3: Validation Results Table

The following grades were used to rank the Information Security Awareness level in an organization that would like to use this model.

- Above 80% would be a '5' which excellent
- Above 70% a '4' which is very good
- Above 60% a '3' good
- Above 50% a 2 is Pass
- Below 50% a '1' is a fail

6. CONCLUSION AND RECOMMENDATION

6.1 Research Summary

This study mainly focused on the niche area of Information Security awareness with the larger area of Information Security. Many studies have been done on Information Security in terms of cost benefit analysis and return on investments. This study took a different approach to study various means utilized to impart Information Security awareness in organizations. The study also realized that measurement of awareness levels in organizations is not often conducted. The study sought to propose an Information Security awareness measurement model that could be adopted by banking institutions. Various factors were considered in the proposed model which was based on a prototype that was developed earlier. The proposed model was modified accordingly in order for it to suit local requirements as dictated by respondents who provided feedback in a survey that was conducted by the researcher. The proposed model was validated with test data through a Microsoft Excel Document. The validation of the model was considered as a success by the researcher.

6.2 Achievements of the study

This study has been able to explore many previous works on the Information Security Awareness Measurement, and from those works, the study was able to help in developing a new information security awareness measurement model that can be used in any stock market around the World. From the validations, it can be stated that the study was a success. Further study on the field is highly encouraged to explore other possibilities in this field of Information Security awareness.

6.3 Benefits of this study

The following are the benefits of this study as outlined below. The overall benefit will be to the research and academics world in terms of a different angle at which to look at the measurement of awareness in organizations as well as a different angle to look at the model to measure awareness levels.

The study brings out clearly the benefits of identifying and making use of measurement of awareness to showcase the organizations overall level of awareness. This would not be possible without the desire and the need to measure for awareness within a respective organization.

Additionally, the management team gains a deeper Insight into organizational risks regarding awareness of Information Security than they would have possibly been able to without the use of measuring of awareness.

This study showcases the aspect of performance at Individual, divisional, regional and organizational levels which can be incorporated into the annual organization performance. This would especially important in organizations that are highly security conscious such as Research firms and Information Security firms.

The proposed model allows the developer to keep tabs on the change in behaviour of their organizations staff. This is especially important for the management since they are now given the leeway to correct any anomalies or gaps by implementing smart training and awareness programs. Positive change in behaviour results in reduced cases fraud and security incidences since the staff are more knowledgeable and informed in Information Security matters.

Allocation of funding, time and staff resources for awareness can prove to be a challenge for some organizations' Information Security teams. This study provided an avenue through which justification for the resources may be done with ease through presentation of solid facts on the performance of the organization as a whole in terms of Information Security awareness.

6.4 Limitations

The most notable limitation in this research is getting access to the security information at the NSE. This is occasioned by the mistrust that comes with the obligation bestowed on to the NSE and the Capital market to safeguard the integrity and privacy of the dealings and information security at the exchange.

6.5 Recommendations

Following the sections discussed in this document, the researcher came up with a number of recommendations regarding the focus area of research which is the measurement of Information Security awareness levels in local banking institutions. The recommendations are in three broad areas:

a) Awareness Measurement is necessary - As documented at various levels of this research and feedback from analysis of respondents, it remains very important for organizations that invest in Information Security awareness activities to also measure the levels of awareness in their organization. This will enable the organization shore up its security status while at the same time providing an indicator of the impact of the awareness activities to the organization.

b) Structured Measurement - Measuring of awareness levels should be carried out in a structured organized manner. This will assist the organization to easily highlight

problematic areas touching n the organization which have a bearing on Information Security. The organization will now be in a position to allocate those specific areas of Information Security with the necessary resources to address them.

c) Awareness levels research - From the literature review, the researcher note d that the area of measurement of awareness levels has not received enough attention compared to the area of awareness activities and their effectiveness. This therefore means that a lot more can be done in this specific area of awareness since it has positive outcomes in relation to the governments' initiatives.

d) New and innovative techniques of imparting awareness are required so as to keep up with the ever changing computing environment. New communication and business operating channels such as the social media, mobile banking, internet banking present most financial institutions with a challenge due to their dynamic nature.

In summary, the process of measuring awareness levels in the organization has minimal impact on resources but its output if utilized properly will result in great positive outcome for the organization in which it has been conducted in:

6.6 Areas of Further Research

This study has reviewed various types of Information Security Awareness techniques used in various previous study. And one thing that can out clearly is that this field of Information security awareness has not been explored in-depth and hence the need to have more specific study on specific individuals in organizations not only in the Capital market but also in all are sectors at large. The suggestion of further tailoring the study on individuals is that when we look at the organization as whole, we are bound to miss one single link which might cost the organization dearly, since individuals make the organization link and the chain as they always say, it's as weak as its weakest link.

REFERENCES

About.com. (2014). *Information Technology Audit*. Retrieved from http://jobsearchtech.about.com/od/historyoftechindustry/g/IT_Audit.htm

Aggeliki Tsohou, S. K. (2004). *Process-Variance Models in Information Security Awareness Research.* Athens University of Economics and Business, Dept. of Informatics, Athens.

Andreas Charitou, U. o. (2009). Market making in international capital markets: Challenges and benefits of its implementation in emerging markets. *International Journal of Managerial Finance, Vol. 5* , pp.50 - 80.

Arief, B. a. (2005). Computer security impaired by legitimate users. *Computers and Security* .

B.T, S. &. (2008). *A Framework for Information Security Management Based on Guiding Standards: A United States Perspectives.* Issue in informing Science and Information Technology Vol 5.

Birks, M. &. (2007). *How to use a questionnaire from.*

Bowden, J. S. (2003). What it is and Why - The Basics. *SANS Institute* .

Christopher Budd, G. B. (2015). *Security Strategies*. Retrieved 2015, from MSDN: msdn.microsoft.com/en-us/library/cc723506.aspx

CMA. (2012). *CMA Internal Control Guidelines.* Nairobi: CMA.

Cynthia Irvine, H. A. (2005). Security Education and Critical Infrastructures.

Denscombe, P. M. (2001). *The Good Research Guide*. Retrieved from Social Research at De Montfort. University.: wansuharyanto.files.wordpress.com/.../martyn_denscombe_the_good_researcg_guide

Engleman, V. d. (2004). Assumptions of variance and process models.

H.A. Kruger a, W. K. (2006). A prototype for assessing information security. *Science Direct* , 289-296.

Hansche. (2001). *Proceedings of the 8th European Conference on Information Warfare and Security.*

Hong, K.-S. (2006). An integrated system theory of information security management. *Emerald Insight* .

Isabella, M. (2009, 2 19). *CMA on the spot over crisis in stock market*. Retrieved 28 6, 2014, from http://www.businessdailyafrica.com

Jiang et al. (2001).

Kankanhalli, A. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management , , 23* (2), 139-154.

Kearney, a. K. (2005). Information Security Awareness and Culture. *BJournal* .

Kearney, K. (2005). A prototype for assessing information security Awareness. *BJournal* .

Kearney, K. a. (2006). Information Security Awareness and Culture. *BJournal* .

Kearney, K. a. (2006). Information Security Awareness and Culture. *BJournal* .

Khan1, B., & Alghathbar, K. S. (2011). Effectiveness of information security awareness. *African Journal of Business Management , 5* (26).

Kruger and Kearney. (2006). IMPROVING INFORMATION SYSTEM SECURITY BY EVALUATING HUMAN FACTORS. *INTERDISCIPLINARY JOURNAL OF CONTEMPORARY RESEARCH IN BUSINESS* , 2.

Kruger, H. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security , 18* (5), 316 - 327.

Landess, D. (2003). Global Information Assurance Certification. *SANS Institute* .

Lebek, B., Uffen, J., Breitner, M. H., & Neumann, M. (2013). Employees' Information Security Awareness and Behavior: A Literature Review. In IEEE (Ed.), *System Sciences (HICSS), 2013 46th Hawaii International Conference.* Wailea, HI, USA : IEEE .

Malhotra & Birks, 2. (2007). *How to use a questionnaire from.*

McCoy, C. &. You are the key to security: Establishing a successful security awareness program. *32nd Annual ACM SIGUCCS Conference on User Services, .* Baltimore, MD, USA.

Merriam-Webster. (n.d.). *College Dictionary*. Retrieved July 1, 2014, from http://www.merriam-webster.com/dictionary/security

NSE. (2014). */about-nse/history-of-organisation.html*. Retrieved May 2014, from Nairobi Securities Exchange: https://www.nse.co.ke/about-nse/history-of-organisation.html

NSE. (2014). *Nairobi Securities Exchange History*. Retrieved Novermber 2014, from Nairobi Securities Exchange: https://www.nse.co.ke/nse/history-of-organisation.html

Oxford. *Oxford Dictionary.* Oxford Dictionary.

Peltier. (2005). Proceedings of the 7th International Conference on Information Warfare.

Point Compass. (2014). *Internal Control*. Retrieved from Compass Point: http://www.compasspoint.org/internal-controls-checklist

professionals., G. d. (2014). *Practical Information Risk Management Process Framework*. Retrieved 2015, from Global Information Assurance: http://www.giac.org/paper/gsec/3303/practical-information-risk-management-process-framework/105444

Rhodes, U. (2015). *Basic Computer Security Precautions*. Retrieved 7 30, 2015, from http://www.ru.ac.za/: http://www.ru.ac.za/informationtechnology/itdivision/policiesandprocedures/security/

Risk Management. (n.d.). Retrieved 3 7, 2014, from Economic Times: http://economictimes.indiatimes.com/definition/risk-management

Rittenberg, L. E. (2009). *Internal Control — Integrated Framework.* COSO.

Rouse, M. (2007, May). *Security Policy*. Retrieved from Search Security: http://searchsecurity.techtarget.com/definition/security-policy

Savola, K. a. (2007). Fulfilling the Needs for Information Security Aware. *6th Annual Security Conference.* Las Vegas NV.

Schneier, B. (2004). *Schneier on Security*.

Shuttleworth, M. (2014). *Research Hypothesis*. Retrieved 7 15, 2014, from https://explorable.com/research-hypothesis

Skaraas, T. a. (2005). Creating a security culture. *TELEKTRONIKK* .

smallbusiness. (n.d.). *Contigency Management Business*. Retrieved 7 2014, from smallbusiness.chron.com : http://smallbusiness.chron.com/contingency-management-business-23285.html

Solutions, V. T. (2015). *Security*. Retrieved 2015, from Vesta Technology Solutions: http://vestatechsystems.com/security.html

Spurling, P. (1995). Promoting security awareness and commitment. Information Management and Computer Security.

Stanton J.M., S. K. (2005). Analysis of end user security behaviours. Computers & Security. *24*, 124–133.

Stanton, J. S. (2003). Examining the linkage between organizational commitment and information security. *Proceedings of the IEEE Systems, Man, and Cybernetics Conference.* Washington, DC.

Steyn, H. K. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security* .

Terms, M. (n.d.). *ATS (automated trading system)*. Retrieved 7 2, 2014, from MoneyTerms: http://moneyterms.co.uk/ats-automated-trading-system/

Tessem, S. (2005). *INFORMATION SECURITY CULTURE IN THE BANKING SECTOR IN ETHIOPIA.*

Teufel, S. a. (2003). A Conceptual Model to Understand Information Security. *International Journal of Social Science and Humanity, , Vol. 4, No. 2*.

Teufel, S. a. (2003). Information Security Management, Education and Privacy. In *Google Books.* Kluwer Academic Publishers.

Times, E. (2015). *Risk Management*. Retrieved 2015, from The Economics Times: http://economictimes.indiatimes.com/definition/risk-management

Trader, A. (2014). *Make Your Distributed System Cyber-Secure*. Retrieved 7 2, 2014, from Automated Trader: http://www.automatedtrader.net/blogs/real_time_innovations_rti/150612/make-your-distributed-system-cyber_secure

Veiga, M. a. (March 2014). A Conceptual Model to Understand Information Security. *International Journal of Social Science and Humanity , Vol. 4,* (No. 2,).

Venkataraman, K. (2001). Automated vs Floor Trading: An analysis of the execution cost on Paris and New York Exchange. *The Journal of Finance, Vol LVI, No. 4* .

Yen-Ping Ch, K.-S. H. (2003). An integrated system theory. *Information Management & Computer Security* , 243-248.

Zakaria, O. &. (2003). A Conceptual Checklist of Information Security Culture.

APPENDIX I:

Research Questionnaire

Part A – General Questions

1. What is the name of the organization? _____

2. What is you gender?

Male ☐ Female ☐

3. How long have you been working in your current organization?

Less than one year ☐ Between 1 and 5 years ☐ Above five years ☐

4. How many employees does your employees does your organization have?

Less than 10 ☐ Between 10-100 ☐ Over 100 ☐

5. Are you an employee or an Stock market Agent?

Employee ☐ Stock Agent ☐

6. If employee what is your current position?

IS Manager ☐ Information Security Manager ☐ System End-user ☐ Other ☐

7. If stock Agent, do you have access to the system?

Yes ☐ No ☐

Part B – General Information Security Awareness

8. Do we have the information security (I.T) team?

a. Yes, we have a company security team. ☐

b. No, we do not have a company security team. ☐

c. I do not know. ☐

9. Do you know who to contact in case you password is hacked or if your computer is infected?

a. Yes, I know who to contact. ☐

b. No, I do not know who to contact. ☐

10. Do you know how to tell if your ATS system password is hacked?

a. Yes, I know what to look for to see if my computer is hacked. ☐

b. No, I do not know what to look for to see if my computer is hacked. ☐

11. Have you ever given your password from work to someone else?

a. Yes ☐

b. No ☐

12. How secure do you feel your ATS password is:

a. Very Secure ☐

b. Secure ☐

c. Not Secure ☐

13. 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. ☐

14. Is your computer configured to be automatically updated?

a. Yes ☐

b. No ☐

c. I do not know. ☐

15. How careful are you when you open an attachment in email?

a. I always make sure it is from a person I know and I am expecting the email. ☐

b. As long as I know the person or company that sent me the attachment I open it.

c. There is nothing wrong with opening attachments.

16. Can you use your own personal devices, such as your mobile phone, to store or transfer confidential 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. 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

b. No

18. Has your boss or anyone else you know at work asked you for your password?

a. Yes

b. No

19. Have you downloaded and installed software on your computer at work?

a. Yes

b. No

20. 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

Part C – Information Security Awareness Techniques

This section is designed to establish the various information awareness techniques employed by the security department to secure the organization information and how effective they are. *(Tick appropriately)*

QUESTIONS	YES	NO

i.	Have you read the Information security policy document?	○	○
ii.	When you were employed/given stockbrokerage agency, were you taken through the Information security awareness program as part of your induction?	○	○
iii.	Have you ever been trained on the Information security awareness by your organization?	○	○
iv.	Are security responsibilities included in the letter of appointment or contract?	○	○
v.	Are information on security awareness included in the existing training materials?	○	○
vi.	Is the information security awareness training mandatory?	○	○
vii.	Have you ever saved your ATS password in your computer?		
viii.	What other information awareness techniques are employed in your organization that I have not listed here?		

22. Give your view to the following questions in regards to NSE ATS. *(Tick appropriately)*

Question		**Strongly Agrees**	**Agrees**	**Neutral**	**Disagree**	**Strongly Disagree**
i.	Do you think there is need to measure information security awareness in your organization?	○	○	○	○	○
ii.	Do you think information security awareness should be carried out in both	○	○	○	○	○

	organization and individual level?					
iii.	Would you be advocate for a random security awareness test amongst all the staff and agents in your organization?	○	◉	○	○	○
iv.	Do you think measuring in information security awareness enhances change in information security behavior?	○	○	○	○	○
v.	Company employees should be taught thoroughly about information security	○	○	○	○	○
vi.	There ought to be more opportunities for information security training at companies	○	○	○	○	○
vii.	Do you see any problems with using a computer that did not have anti-virus software installed?	○	○	○	○	○
viii.	Do you think it is acceptable to break rules as long as no problem occurs?	○	○	○	○	○
ix.	Security measures reduce user-friendliness	○	○	○	○	○

23. What problem do you think affects the Information Security Awareness within your organization?

i. Information security awareness is not a priority in my organization.

ii. Lack of information awareness content

iii. Lack of time

iv. Lack of resources at my organization

24. Would you support outsourcing of information security awareness from another organization specializing in IT security?

i. Yes

ii. No.

iii. Not sure

25. Do you think there is need to Measure Information Security Awareness?

i. Strongly Agrees

ii. Agrees

iii. Neutral

iv. Disagree

v. Strongly Disagree

26. Would you be willing take a vocabulary test to Measure Awareness levels?

i. Strongly Agrees

ii. Agrees

iii. Neutral

iv. Disagree

v. Strongly Disagree

27. What would you like to see as the scope of measuring Information Security Awareness levels?

i. Cover levels of the NSE where Information is involved

ii. Only critical areas of ATS

28. From which region are you based at?

i. Nairobi Region

ii. Central Kenya

iii. Western Kenya

iv. Coastal region

v. Eastern Kenya

vi. Northern Kenya

vii. Other *(Indicate)*_____

29. What levels of Awareness would you desire implemented?

i. Staff has internalized information security awareness knowledge.

ii. Information security awareness has gained general acceptance among the staff members

iii. Staff intention has been drawn towards information security awareness.

30. Which of these Information Security Awareness Metrics would you prefer?

i. Number of request to security department

ii. Number of hits to security information web page

iii. Percentage of weak password users

iv. Percentage of illegal traffic on the internal computer network

v. Percentage of paper waste shredding

vi. Percentage of employees having a clean desk at the end of the day

vii. Number of reported information security incidents

viii. Percentage of employees who have finished the security training

31. Which method of measure would you advocate for in measuring the awareness based on organization structure?

i. Structure based awareness level where sections are scored individually

ii. A holistic company based awareness level where the organization is measure as one entity

iii. Regional based awareness where different regions are scored individually

iv. All of the above

PART D:

Information Security Awareness Quiz Review Questions:

Question 1:

Information assets are:

a) Computer data items, often in databases

b) Valuable items of personal and proprietary information

c) IT systems and networks

d) A mythical invention by accountants

Question 2

The computer tells you your pass word has expired and needs to be changed. You should:

a) Pick the same pass word as before, only with a number on the end

b) Ask a friend to check if your pass word is strong enough

c) Call the IT Help/Service Desk to log a support call

d) Pick along pass word or pass phrase that is quite different to the previous ones

Question 3

An important incoming email from a colleague has been quarantined by the antivirus software. You should:

a) Ask the person to re-s end the email this time to your Yahoo email address

b) Call the IT Help/Service Desk for assistance

c) Run a full virus scan immediately and check all your data backups' for viruses too

d) Call the customs and immigration authorities

Question 4

What does information security mean to you?

a) Frustration

b) Annoyance e

c) Inconvenience

d) Protecting me, my job and my future

Question 5

If an IT person working on your PC asks you for your password, you should:

e) Make up a fake password on the spot

f) Refuse to disclose your password and report this as a security incident

g) Tell them your password because they are from IT

h) Tell them someone else's password

Question 6

The system tells you your password has expired and needs to be changed. You should:

e) Pick the same password as before only with a number or a month on the end

f) Ask a friend to check if your password is strong enough

g) Call the IT Help/Service Desk to log a support call

h) Pick a long password or pass phrase that is completely different to the previous ones.

Question 7

An important incoming email from a colleague has been quarantined by the antivirus software. You should:

e) Ask the person to re-send the email to your Yahoo! email address

f) Call the IT Help/Service Desk for assistance

g) Run a full virus scan immediately and check all your data backups for viruses too

h) Call the customs and immigration authorities

MALWARE:

Question 1

A friend emails you unexpectedly at work with a "cool computer game". You should:

i) Run the game to see just how cool it really is Run, just run

k) Call your friend to find out more about the game

I) Ignore or delete the email as this is not appropriate for work

Question 2

Someone seems to have "done something" on your PC, and now annoying and sometimes disturbing popup messages keep appearing. You should:

i) Call the IT Help/Service Desk to report an incident

j) Ask around to find out who has been using your PC, and tell them to sort it out

k) Ignore the problem as it will probably go away all by itself

I) Activate the antivirus software and run a full computer scan

Question 3

The popup s are gone but your PC is still behaving a little oddly. You should:

i) Call the IT Help/Service Desk to report an incident

j) Ignore it and carry on regardless

k) Start Task Manager to find out what programs are running

I) B e glad that it's only a little odd to day

True/False Questions

Question 1

W hen changing passwords it is OK to repeat the same password every third time it is changed.

False - No, a repetition cycle of three months is a fairly recognizable pattern. Most large systems will require you to use at least twelve different passwords before a password can be repeated.

Question 2

It's OK to use consecutive letters on the keyboard so long as the letters are random, as an example,

QWERTY would be a good password.

False - No, although the letters are alphabetically random they are consecutive on the keyboard. They are also easy to spot if you watch someone enter them on a keyboard.

Question 3

I can be held responsible for anything that happens if someone else used my password.

True - the system only knows you by your logon and password. If someone else used your logon and password the systems thinks it is you and any inappropriate action is attributed to you.

Question 4

It's OK to logon a terminal with my password in the morning and let my colleagues use the terminal anytime that they need to.

False - No, The purpose of a unique logon and password is to identify you to the system and to provide accountability. If you logon to your system and allow others to used it you will be held accountable for any inappropriate activity that takes place on that terminal.

Question 5

Social engineering is the intentional manipulation of an individual into believing that the Information requester is authorized and entitled to receive information.

True - Social engineers can be very convincing. Be careful of people calling asking or requesting confidential information if there is any doubt, ask for their name and phone number. If you believe someone is using social engineering tell your supervisor.

Question 6

When we talk about the confidentiality of information we are referring to the manner of disclosure.

True - Privacy of information refers to the issues surrounding the disclosure of information.

Question 7

It's alright t o use my car's nick name as a pass word since no one knows my car 's nickname.

False - You should not use a family member's name, a pet s name, the name of a hobby, consecutive letters on the keyboard (qwerty), etc . In normal casual conversation we will mention these names to our acquaintances. As a result, it is first thing a hacker will use to gain en try to your system.

Question 8

My NSE email is private and no one can look at it

False - The company email system is owned by the company and they are allowed to scan your email for inappropriate use or suspected policy violations

Question 9

A hardware key logger is a hardware device that captures keystrokes on their journey from the keyboard to the computer.

True - Used mainly to collect Password Information.

Question 10

Spyware is software that comes hidden in free downloadable software and tracks your online movements, mines the information stored on your computer, or uses your computer's CPU and storage for some task you know nothing about.

True - Used mainly to collect information from a users' computer that can be used for identity theft.

Question 11

Adware is software to generate ads that installs itself on your computer when you download some other (usually free) program from the Internet)

True - Adware are usually responsible for all the pop up adverts on an infected Machine. Inform IT Helpdesk to remove them.

Question 12

A worm is written with malicious intent to cause annoyance or damage.

True - A worm spread throughout the network at lightning speed with the intention of jamming the network with unnecessary traffic.

Additional information

Which two strategies will help protect hard copy information? (Choose two.)

a) Shred printouts before disposal.

b) Encrypt all files.

c) Sign all documents.

d) Adopt a "clean desk" policy.

Hard Copy Reading Information

Hard copy Information refers to printed Information. Can be in form of emails, reports, analysis documents, financial figures etc.

Solution: Main means of protecting Hard Copy Information is:

- Shred printouts before disposal- make use of shredder

- Adopt a "clean desk" policy - Do not leave any documents on your desk unattended when out of office.

Which negative outcome can result from hoax virus warnings and malicious spam?

a) Denial of service.

b) Data loss.

c) Reduced account privileges .

d) Credit card fraud.

7. APPENDIX 2

7.1 Letter of Introduction