THE UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING AND INFORMATICS

# TECHNOLOGY SUPPORTED WEB-BASED IT SECURITY AWARENESS TRAINING

BY

NDIBA DANIEL KIMANI

P53/79748/2015

SUPERVISED BY: DR. EVANS MIRITI

**Thesis Submitted for Examination in Partial Fulfilment of the Requirements for Award of the Degree of Master of Science in Distributed Computing Technologies of the University of Nairobi**

**2018**

# DECLARATION

I declare that this thesis is my original work and has not been submitted elsewhere for examination, award of degree or publication. Where other people's work or my own work has been used, this has been properly acknowledged and referenced in accordance with the University of Nairobi's requirements.

Signature: ______________________________ Date: ______________________

**Daniel Kimani Ndiba**
**P53/79748/2015**
School of Computing and Informatics
University of Nairobi

This thesis is submitted for examination with the approval of research supervisor:

Signature: ______________________________ Date: ______________________

Dr. Evans Miriti
School of Computing and Informatics
University of Nairobi
P.O Box 30197 – 00100
Nairobi – Kenya
eamiriti@uonbi.ac.ke

# ABSTRACT

Research has indicated that a significant portion of information security breaches in Organizations are caused by employees, whether intentional or non-intentional. To mitigate this, organizations have set-up ICT security awareness programs. These awareness programs are meant to empower employees with knowledge and skills that enable them identify, prevent and know how to react to potential information security incidents. However due to lack of standard metrics that measure impact of awareness initiatives, insufficient delivery methods, awareness material content generalization and lack of standard metrics for tracking delivery and deployment, it has become difficult for organizations to monitor, measure and appraise the success and effectiveness of the ICT security awareness program.

It is therefore essential to have a diverse ICT Security Awareness Program with a set of methods to deliver, assess, educate, reinforce, and measure its effectiveness. This study discusses how this can be accomplished by using technology to automate and reinforce a comprehensive Security Awareness program that will meet the above needs. The research aims to investigate the effect of simulated phishing attacks on the motivation of users to undertake a security awareness training and demonstrate how metrics derived from the automated solution can be used to measure the levels of security awareness in an organization.

In this study we conducted weighted surveys through online questionnaires on staff in an organization that uses PowerPoint presentations for their awareness program. The survey questions were designed to measure a set of basic characteristics of the organization's security awareness posture; it provided several metrics to measure the risk and awareness levels in an organization. We also ran phishing simulations targeting employees. The simulations were able to identify which users fell victim and clicked on the phishing emails and also showed that users who fell victim proceeded to undertake the online Security awareness that was initiated thereafter the successful attack. This empowered staff to be familiar with the most common attack scenarios in the simulation, and the awareness training thereafter empowered them with countermeasures to take, that can prevent them from being compromised. The study also provided management with visibility on the most vulnerable staff and departments, where awareness training should be focused and intensified.

# TABLE OF CONTENTS

## LIST OF TABLES

## LIST OF FIGURES

# CHAPTER I - INTRODUCTION

## 1.1 Background

There is an extensive array of threats to information security, for example, human errors, robbery, employee sabotage and treachery, natural catastrophes, technical failures, malicious cybercriminals etc. As indicated by (Whitman and Mattord, 2005) employee errors, whether intentional or non-intentional, are ranked among the top risks to information resources. ICT security training and awareness are a part of the procedures adopted by organizations to teach staff on ICT security and reduce the risk posed by employees.

Over the years, research has indicated that in an organization's cyber security strategy, humans are a critical component of the security plan; the attackers have figured out that the most vulnerable portion of the company is the people. Vulnerabilities in technologies and computing infrastructure can be mitigated by applying hardened configurations and patching software vulnerabilities; however, you cannot apply a patch to human ignorance (SANS, securing the human, 2015). The security culture of an organization if weak can make an organization much more vulnerable to Security Breaches and Data Leakages. Many attack types nowadays rely on human intervention to succeed.

This human factor in data security is mostly tied to human behaviour and human learning. This implies that employees who are entrusted by their organizations to interact with high value information assets, for business driven operations, should behave in a manner that safe guards the security of the organizations IT assets; and also need to have the required knowledge about cyber security-related incidents. (van Niekerk, 2005).

Numerous Global Security Standards including ISO 27000 have highlighted criticality of organizations carrying out security awareness. In the Banking Sector in Kenya, the Central Bank of Kenya (CBK), which is the regulatory body for banking institutions in Kenya, also released a Cyber Security Guidance note for the banking sector. One of the key requirements mentioned is the need for Banking Institutions to conduct ICT Security Awareness.

According to (Gaunt,2000) he discusses that in spite of the understanding that awareness is essential, we cannot be certain that a reasonable message is being conveyed to the consumers. This is particularly valid for dynamic and complex types of attacks like phishing assaults which can be very vague to describe.

Training on security awareness should impact all representatives inside an institution to guarantee the proper conduct is followed by all and subsequently accomplish consistence to cyber security strategies. To affirm this, the following accompanying inquiries need to be answered: what kind of security awareness training will effectively impact behaviour i.e. how imperative is the nature of the awareness material and the method of conveyance? How can IT security experts all the more effortlessly convey the awareness message to guarantee more prominent support from end-users? As far as awareness training, additional institutionalized instruments ought to be investigated to decide how best to quantify understood information.

With so much emphasis placed on Information Security Awareness, in this study a review of Security Awareness literature has been conducted towards revealing applied theories, Information Security awareness perspectives, concerns, benefits and problems or gaps that may promote or inhibit its successful implementation. An understanding of current security awareness methods was sought with a view of investigating how technology may facilitate to improve the process.

In this study, we investigate the effect of a simulated phishing attack on the motivation of employees to undertake security awareness training. We present the results of the phishing attack simulation, click results showing employees who fell victim and thereafter trace those that proceeded to undertake security awareness training after a successful attack. In the results and discussion, we shall indicate how the results can be used as metrics to track participation in security awareness, measure awareness levels and identify which populations, departments are most vulnerable and require targeted security awareness training.

We also conduct an investigation using a weighted survey. The survey consists of 26 questions designed to measure a set of basics characteristics of the organization's security awareness posture. Some questions collect factual data (role, location) while others collect data about the user's awareness, attitudes and behaviours. It gathers behavioural data on how users respond to threats, as well as data on attitudes and perceptions of organizational culture. We presented results on how this can help security training and awareness professionals gain a richer, more informed understanding of users' attitudes and habits within the context of their activities.

## 1.2 Problem Statement

Information security researchers have conveyed that a weak Security Culture makes an organization much more vulnerable to Security Breaches, Data Leakage and General Organizational Exposure to attacks as people are a key link in Securing Company Information assets.

Modern organizations must ensure that security awareness is one of the pillars of their cyber-security strategy. Most organizations have recognized this threat, and to be able to combat it, organizations have begun setting up Information Security Awareness programs, in line with recommendations from globally recognised Cyber Security Standards bodies such as ISO 27000 and National Institute of Standards and Technology (NIST) cyber security framework.

However current awareness programs utilizing PowerPoint presentations and email communications still face several challenges as discussed below:

Lack of metrics that measure impact of awareness initiatives; PowerPoint presentations and email broadcasts convey the security awareness message, however they do not provide a standard metric or tangible measure that can be used to show that the message has impacted the target user and delivered the intended message.

Security awareness material content generalization; most of the Security awareness material used in security awareness is generalized and not specific to organizations and departments. A PowerPoint presentation downloaded online contains general material, however different organisations and different departments have different information security needs and dynamics, particular departments require more focus due to their sensitivity. It is therefore necessary to identify these target groups and select content which will be applicable to them.

Insufficient Delivery methods; Security professionals convey awareness initiatives and teach end users, we however tend to overlook the complexity of the information we are passing, and the capacity of the trainees to comprehend the risks. We must therefore look for innovative non-conventional strategies to convey the awareness message. We need to get our users more engaged to ensure they read, understand and most importantly retain the material. We also need to enforce exercises to practice it. This will guarantee we are putting in more work on the nature of awareness materials that we introduce.

Lack of metrics for tracking delivery and deployment; Conveying and tracking who finishes security awareness activities can be an excruciating procedure and very time consuming. It would normally involve participants signing off on participation sheets which should then be captured and tracked on an excel sheet. This requires manual input and follow up to track who has attended the required training sessions. We also have cases of the signed attendance sheets being misplaced during filing and storage. This procedure works, however it is prone to human error, extremely monotonous, and not feasible especially in an organization with a large number of people.

## 1.3 Objectives

### *1.3.1 Main Objective*

The main objective of the study was to investigate the impact of technology through a simulated phishing attack on the motivation of users to undertake security awareness training.

### *1.3.2 Specific Objectives*

1. Develop a phishing attack simulation system that can be configured to send phishing emails based on different templates, at different targeted users and linked to an e-learning platform that launches after a successful phishing attack.
2. Conduct a weighted survey with questions designed to measure a set of basic characteristics of the organization's security awareness posture and provide several metrics to measure the risk and awareness levels in the organization.
3. Demonstrate how the results of the phishing attack simulations can provide metrics to measure awareness levels in an organization, impact, participation et al; this may include percentage of staff who clicked, identifying most vulnerable staff/departments, identify percentage of successful victims that have taken part in the awareness training et al.

## 1.4 Justification and Significance

### *1.4.1 Justification*

Research has indicated that there is a common misconception that cyber security is all about technology (Dutton, 2017). Organizations have invested in assortments of hardware and software. Technology is indeed a very critical part of cyber security, but alone it is merely not enough to protect an organization from modern cyber threats. Effective and robust cyber security strategy needs to be built on three key pillars- people, processes and technology; (Lappin, 2017).

The people element of the three pillars is often neglected but important to consider. Everyone in the business needs to be aware of their role in preventing and reducing cyber threats. Cyber security is a business issue and everyone has a role to play. An effective security awareness programme can help reduce the risk of cyber threats aimed at exploiting people. (Dutton, 2017).

According to (Gaunt,2000) in spite of the understanding that awareness is essential, we cannot be certain that a reasonable message is being conveyed to the consumers. Especially for dynamic and complex types of attacks like phishing assaults, how the material is conveyed is very critical for success to ensure that the message is driven home.

Research conducted on information security has customarily been inclined towards specialized parts of security like encryption, intrusion detection, PKI et al. However, measuring the viability of security awareness, procedures of conveyance and inspecting behavioural angles have been to a great extent disregarded. (Stephanou and Dagada, 2013). This gives a decent zone for additionally research.

### *1.4.2 Significance*

Employees are frequently under attack from malicious phishing emails, browser based attacks, mobile device and USB device based attacks, social engineering among others. This brings about the need for an intuitive technology driven awareness training platform that can enable staff to interact with and comprehend the components of such attacks and apply this learning in their everyday activity, (Perry, 1985).

As discussed by (McCoy and Fowler, 2004) cyber security experts within organizations have put in place IT security awareness campaigns in their organizations. However, they have no real way to gauge the adequacy of their efforts and the impact of the awareness initiatives. The developed solution will put in place metrics that help them report on the adequacy, progress and impact of the security awareness. It will also help them track on attendance and enable them identify which particular business units are most vulnerable and may require focused training.

Financial institutions are often required by regulators, auditors and internal policies to demonstrate that they have conducted IT Security Awareness. For instance, in the Kenyan banking sector, the CBK guidance note, 2017; requires that banks conduct employee IT Security Awareness training and should provide evidence of the same when needed. Researcher and analysts such as (Sommers, K. Robinson, B, 2004) have argued that conveying and tracking who finishes security awareness activities can be an excruciating procedure and very time consuming. However, with the developed solution in place, management can easily pull this information as reports from the automated solution and demonstrate that they have a current Security awareness campaign in place.

# CHAPTER II – LITERATURE REVIEW

This chapter will present a background discussion on Information Security Awareness, describing its growing importance, planning considerations, steps that have been made towards adopting Security Awareness and some of the challenges that have been faced in implementing such programs. The discussion involves insight from publications from previous researchers and technologist who have also delved into that area. I will further describe the evolution of Security Awareness from a traditional classroom exercise to more versatile interactive program that should take advantage of automation and web-applications and services.

From the accessible research, different branches identifying with data security awareness examine right now exist. The scene of data security mindfulness research can be sorted as takes after: (Stephanou & Dagada, 2013)

Figure 1 shows one way of trying to understand of the accessible research material for information security. You will find that most of the research work will likely be placed into one of the below categories. In my study I focus mainly on research on the importance and techniques of Security.

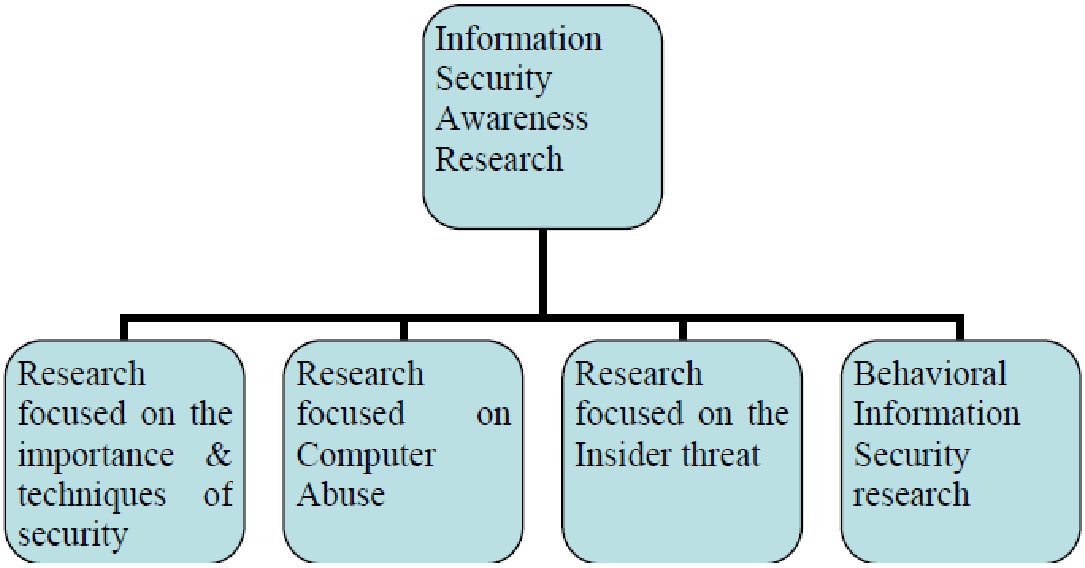

Information Security Awareness Research
Research focused on the importance & techniques of security
Research focused on Computer Abuse
Research focused on the Insider threat
Behavioral Information Security research

***Figure 1 Information Security Awareness Landscape***

## 2.1 Theoretical Literature Review

### *2.1.1 The growing importance of a Security Awareness program in an organization*

In the rising web knowledgeable society, security vulnerabilities by means of exceptional online social exercises e.g. Facebook, blogging, texting, YouTube., and so forth.; are developing exponentially. Clients taking part in these online exercises have differing and unequal levels of security awareness. The uniqueness in security awareness has brought about feeble lines of safeguard. Additionally, exasperating the powerless line is the ceaseless advancing of dangers and assaults that can evade the generally acknowledged security innovations we know like hostile to infections, antispam programming, and firewalls; (Claburn, 2005). Accordingly, the change of security awareness levels of general clients should be one of the present best security concerns. If not, regardless of what amount refined security innovation is sent, a little human mix-up like discharging classified data to noxious aggressors; or interfacing a corporate tablet to unsecured remote systems in a ; or losing a versatile USB drive containing delicate organization data can transform these advances into vulnerable targets.

With distributed services and peer-to-peer associations becoming normal acceptable online social practises, data security can never be focused on enough. Noticeable web-related security dangers go from taking client ids and passwords to characterized spamming, to protection interruption, to copyright infringement. Even for the institutions whose users are not effectively engaged with an online social activity, security dangers like identify theft, privacy protection, password assurance, and so forth.; relentlessly exist.

Users with low security awareness are regularly imprudent in dealing with sensitive and classified data (Schneider and Therkalsen, 1990) . The wellspring of security dangers can begin from software, equipment, physical lapses, specialized attacks, and lack of knowledge on security policies etc. It is basic that an institution trains users to know about potential security risks, how to identify them and taking remedial activities if attacks do happen. (Harris and Chen, 2009).

### *2.1.2 Measuring/Evaluating ICT Security Awareness in an Organization*

One of the basic security awareness success components is how to assess its adequacy. As a beginning step, certain criteria on which estimations will be taken require to be distinguished.

These key criteria are vital to guarantee that areas, vital to all stakeholders, shape the premise of a measuring apparatus. It will moreover offer assistance to centre questions, or viewpoints to be measured, when creating for case a study instrument. A value centered approach that will take into account stakeholders' wishes, concerns, issues and values relating to data security awareness, is recommended for identifying the key criteria ranges.

Once the key criteria have been recognized, employees ought to be reviewed to identify their level of awareness. This strategy was based upon research by (Kruger & Kearney, 2006) and is portrayed by them as takes after.

It makes utilization of procedures acquired from the field of social brain research that recommend that educated inclinations to react in an ideal or negative way to a specific question have three parts: influence, conduct and perception. The influence segment includes one's certain and negative feelings about something; the conduct segment comprises of an expectation to act in a specific way while the cognizance segment alludes to the convictions and contemplations one holds around a question (Feldman, 1999; Michener and Delamater, 1994). These three parts are utilized as a premise and the model is to be created on three comparative measurements specifically what a man knows (information); how would they feel about the point (mentality); and what do they do (conduct). This approach isn't totally new and different scientists have just performed work where the sociologies were identified with the field of data security awareness. Thomson and von Solms (1998) have indicated how social mental standards could be used to enhance the viability of a data security awareness program while Schlienger and Teufel (2003) made utilization of social-social measures to characterize a model for investigating data security culture in associations.

Notwithstanding the representative studies, suitable framework created information ought to likewise be utilized as contribution to the last model. This information will help with the assurance of security conduct. Framework information is required to be more solid (not subjective or human ward) and ought to be genuinely simple to get.

### *2.1.3 Online/E-learning systems as a feasible means to deliver Security Awareness programs*

Numerous clients find existing Security Awareness programs exhausting and inadequate (Leach and Behaviour, 2003). The Web is a perfect vehicle to convey online Security programs to conquer the learning insufficiency. Course materials in advanced configurations can be diverse to the point that they can be produced to raise the learning interests of users in view of their needs. The retrieval of course materials can be amongst educator and users, or multilateral, among at least two users. A powerful Security Awareness program intensely depends on both the "push" and "draw" of important and convenient security data to and from users. (Harris and Chen, 2009).

As e-learning frameworks turn out to be more refined, they hold numerous potential outcomes of conveying successful and financially viable Security Awareness programs. Human PC interface is an imperative component in the outline of a compelling Security Awareness program. Fusing HCI criteria into the outline of Security Awareness projects can improve their ease of use and learning viability (Johnston, Eloff, and Labuschagne, 2003).

Preparing workers in an e-empowered learning condition has been appeared to have the below preferences:

**1. Flexibility**

This identifies with the area, timing and usage of preparing and appraisal.

**2. Sophistication**

Web based learning and evaluation innovations give more modern approaches to students to interface with content.

**3. Innovation**

Technical advances, for example, cell phones, tablet PCs, reproduction and gaming innovation catch the creative ability of improvement specialists and prompt new and inventive methods of learning and appraisal.

**4. Value for money**

At the point when executed the correct way, learning innovations can influence significant commitments to an association's base to line. Towards Maturity, an association that works with managers to execute and benchmark e-learning capacity, has discovered that associations that have actualized learning advances are detailing a normal cost sparing of 18%. Those associations utilizing more develop learning advances are additionally announcing a 20% change so as to competency (Minchington, 2011).

## 2.2 Empirical Literature Review

### *2.2.1 The influence of media richness on the effectiveness of online SA programs*

Media richness, including sound, gushing video, intelligent blurbs and virtual augmentation are picking up fame in Security Awareness programs (Harris and Chen, 2009). The limit with regards to data abundance of media can be expanded by controlling at least one of the accompanying traits: "(1) The medium's ability for prompt criticism, (2) The quantity of signals and channels accessible, (3) Language assortment; and (4) how much focus is centered around the beneficiary" (Daft and Lengel, 1984).

More prominent social presence of medium impacts a superior cognitive ability for the planned clients and creates a warmth to the correspondence which makes for a superior learning condition. As one of the four characteristics is expanded, the capacity of the media to convey more data and henceforth viably change the comprehension of clients about the considered subjects is expanded.

Face to face gatherings happen to be the wealthiest media since they consolidate the greater part of the properties. Online media have lesser wealth when contrasted with up close and personal gatherings. Notwithstanding, online devices are rising to upgrade media wealth. They incorporate, texting, feeling symbols famously known as emojis, audibles, sound and video transmissions. Blogs have also turned out to be extremely well known in the World Wide Web 3.0; they figure out how to incorporate hypertext, pictures, and offbeat input. Another great illustration which has turned out to be an exceptionally accommodating learning asset is YouTube, YouTube enables the distributed sharing of video documents.

Numerous property organizations are utilizing virtual augmentation to give a mimicked voyage through the whole house for forthcoming purchasers. Auto firms are additionally absorbing the 360 level of virtual augmentation to enable purchasers to view the inside and outside parts of an auto-mobile. (Harris and Chen, 2009)

In the planning and execution of an efficient online automated Security Awareness program, the significance of media and data richness can be critical to success.

### *2.2.2 Phishing for user security awareness*

Educating and training employees on security is amongst the most essential parts of an associations security strategy. Utilizing security activities to strengthen this perspective is as commonly use in the education and security industry alike; (Dodge, Carver, and Ferguson, 2007).

Security awareness is an irregular variable that is exceptionally hard to describe because of user's individual nature. Users make an open secondary passage into our corporate systems through their web empowered services, external applications, and electronic communication with different employees. This weakness is expanded from versatile frameworks that join home and other business systems.

A standout amongst the most widely recognized communications clients have with elements outside control of our nearby systems is email. The July 2006 report issued by the Anti-Phishing Working Group revealed 23,670 exceptional phishing endeavors focusing more than 14,191 sites used to submit wholesale fraud, misrepresentation and different pernicious movement. These sites are exceptionally powerful in nature, existing just for a normal 4.8 days (Anti-Phishing Working Group, 2006). Security mindfulness programs have made a decent showing with regards to of alleviating this hazard, yet the issue remains how to gauge or confirm that clients have comprehended and reliably apply the prescribed procedures they are presented to amid occasional classroom trainings? (Avoid, Carver, and Ferguson, 2007) .

The utilization of activities to strengthen ideas in an instructive setting has been composed about as often as possible (Dodge et al., 2005). The United States Military Academy (USMA) has been exceptionally dynamic in executing hands-on activities, for example, the Cyber Defense Exercise (Dodge et al., 2003). Normally, these activities include investment by knowing members and include a system assault/guard situation. The USMA Academy took the idea of a dynamic learning and built up an email phishing exercise with the goal of assessing the adequacy of our user Security Awareness preparing. (Avoid, Carver, and Ferguson, 2007) .

The activity was named Carronade after the Navy gun utilized as a part of the mid-1770s. Its use hostile operations amid the 1700s, the goal was not to sink an adversary vessel but instead to abstain from harming the body in order to catch it as in place as could be allowed, so it would be held as a "prize". In keeping in accordance with the military subject, this activity is named the Carronade in light of the fact that; while the email can possibly be ruinous, the aim was to get the consideration of cadets associated with the email work out, not to make harm the Academy arrange or to punish the cadets. (Avoid, Carver, and Ferguson, 2007).

Moreover, USMA has partaken in the University of California in an activity called Capture the Flag. (Vigna, 2003) The University felt that the understudies who partook in these digital barrier style practices have a high comprehension of the effects of poor client PC propensities. In any case, the activities just included an example number of understudies. This left alternate understudies whose exclusive presentation to data frameworks security is the yearly old school security mindfulness and preparing program. There exists no formal component to assess the accomplishment of these projects. The advancement of the email phishing exercise was in guide reaction to an issue of how well their client mindfulness programs function.

The diary article "Phishing for client security awareness" by (Dodge, Carver, and Ferguson, 2007) indicates how the group builds up a phishing exercise. They have taken the idea of utilizing an activity and adjusted it in application to assess a client's affinity to react to email phishing assaults in an unannounced test.

### *2.2.3 Evaluating ICT Security Awareness*

In the previous section we discussed that one of the approaches to gauge the value and efficiency of IT Security awareness is assessing and measuring. This can highlight a lot of the success factors required for an IT Security Awareness programs.

A few analysts have gone further to research and concoct structures that can be utilized to gauge IT Security awareness. Schlienger and Teufel, 2005 expressed that assessment ought to dependably be the last advance in an ICT security administration program with a specific end goal to acquire data on the proficiency and adequacy of activities, to characterize follow-up activities and to legitimize interests in the program. While trying to add to the assessment procedure of an ICT security awareness program, the recommended structure was produced by (Kruger, Drevin, and Steyn, 2009), to help with administration of this assignment. The system was created mutually in a scholarly situation and at a private venture and shaped piece of a progressing research process. It incorporated the distinguishing proof of regions to be assessed utilizing an esteem centered approach, and a few remarks on conceivable framework created information that might be utilized to help with the assessment of security conduct of clients. (Kruger, Drevin, and Steyn, 2009).

The value centered approach was a choice system recommended by Keeney (1994) and included four stages.

To start with, interviews were led to decide partners' desires, concerns, issues and so forth inside the choice setting. Next, the aftereffect of the meetings, which spoke to a rundown of individual esteems and wishes, were changed over into goals. These comprised of a choice setting, a question, and a heading of inclination that one needs to endeavour towards (Nah, Siau and Sheng, 2005). Thirdly, a procedure to recognize means and principal destinations was performed. In the event that a protest bolstered or accomplished another target, it was named a methods objective. Else it was a principal objective. At last, the methods and central destinations were sorted out into a system that demonstrated the interrelationships among all targets. The system could then be utilized to infer cause-impact connections and to create choice open doors.

The value centered speculation approach has just been connected effectively in various regions. Hassan (2004) connected it to the natural determination of divider structures, while Nah, Siau and Sheng (2005) utilized the way to deal with depict the estimation of portable applications. Different illustrations can be found in Dhillon and Torkzadeh (2001) and Dhillon, Bardacino and Hackney (2002) where the value centered deduction approach was utilized as a part of appraisal of data framework security in associations and protection worries for Internet business individually.

## 2.3 Major challenges with the existing SA programs in enhancing SA levels of users

Poor security conduct of numerous clients has added to numerous security breaches. Institutions are beginning to perceive the significance of having an ICT Security Awareness program set up. For a Security Awareness program to succeed, it is intrinsic to guarantee that workers accomplish three levels of mindfulness as talked about above in the mental standards: disposition, learning and conduct. As more workers of an association gain ground along these three levels, the general population part of security can be uplifted.

Institutions ought to however take note of that the one-estimate fits-all approach at both the association level and the individual-level has added to the fluctuated execution of Security

Awareness programs (Valentine, 2006). It is fundamental to have a steadier system to tailor a Security Awareness program in light of the levels of security attention to be accomplished.

"Most organizations have accepted that an arrangement of undefined objectives exists for their security awareness program, however they have not really recorded these targets. The final product is an expensive, dubious mindfulness program in view of convention, individual judgment and impulse. This approach isn't endured in some other period of IT security operations and ought not go on without serious consequences in the domain of security mindfulness." (Walls and Gartner, 2013).

"Gartner customers report that numerous representatives acknowledge the substance, structure and conveyance techniques for security awareness trainings to be old fashioned and symptomatic of a security program that is withdrawn from the modern workplace." (Walls and Gartner, 2013) "User aides and arrangements are loaded with articulations that are non-particular and expect clients to take security activities that are past their abilities." (Gartner, 2013)

Some the critical achievement factors for a Security Awareness program are: significance, convenience, and consistency of ICT security information. This is on the grounds that data hazard profiles change constantly (Kruger and Kearney, 2006). Similarly, imperative is the conveyance of the most recent security data in various structures like bulletins, video, courses, simulations and lectures with the goal that clients get a wide range of messages. As web based learning advances, including web-administrations gain quick ground; a considerable lot of its highlights are turning into an achievable other option to convey Security Awareness programs.

In the conventional method for conveying Security Awareness programs, challenges show up when attempting to understand the genuine adequacy of a Security Awareness (Valentine, 2006). A noteworthy test is the absence of a completely created system and stages to convey them. This study tries to address that through a complete online stage.

### 2.4 Discussion of findings and gaps

It is quite evident from previous works that indeed Security awareness is key for any organization. Many of the Cited works agree that Information Security awareness is indeed critical for the Security Posture of an organization. With the growing use of the internet, social media, Internet Messaging and peer-to-peer applications, organizations can no longer rest easy by Investing in high cost security infrastructure like Firewalls, IDS/IPS, anti-viruses etc. The human aspect has to be addressed and addressed effectively.

Using of highly rich media as discussed above may influence how users react to security awareness training. I therefore agree with the hypothesis above and propose that my automated solution should use highly rich media which combines instant messaging, emotion icons popularly known as emoticons, audibles, audio and video transmissions, hypertext and multimedia. The platform should be able to integrate the different forms of media without impacting the performance of the solution. We can recreate attacks from end-to-end so as to show users how they are targeted, the extent to which it may go and for them to understand the extent of damage and impact it has to the organization. It is not enough to give users information, but allowing them to see and understands makes them more likely to react positively to awareness. This can be achieved through multi-media channels, videos and infographics, animations and Augmented Reality Simulations.

Measuring and evaluating security awareness is also seen as a major drawback of the traditional security awareness training. Previous studies have recommended several ways of measuring and evaluating. Amongst one the methods captured above is System generated information and using a value based approached. The frameworks for value based can be enhanced or modified into architecture to be used in my web application. System generated data can then be used in my proposed solution by integrating it with company firewall logs, internet traffic, application data, Anti-virus reports amongst others. These give statistical and factual data on user activity and show which users are posing the highest risk to the organization.

Phishing is one of the most common surfaces for attacks nowadays. A phishing email or scheme will usually give the information an attacker is looking for to enable them launch an attack. Studies have shown how phishing attacks have been used to test level of Security awareness in the Military and Academic Fields (Dodge, Carver, & Ferguson, 2007) .

By building into the integrated web solution, phishing templates and platforms which can be used to periodically target users, we will be able to test how users react to phishing attempts without giving them a prior notice. Users who fall victim to the simulated attacks can then be mandatorily enrolled into a Security Awareness Program.

Research completed on data security has generally been inclined towards specialized parts of security like encryption, interruption identification, PKI et al. Measuring the viability of general security mindfulness and looking at behavioral angles have been to a great extent dismissed.

E-learning has been appeared to be a successful technique for conveying data, information and skills by utilization of computer and Internet innovations to convey a wide exhibit of arrangements that empower learning and enhance execution.

However not much research has been done on the use of e-learning in Security Awareness Training. This is an area that requires further research. This presents an opportunity to study how well e-learning methods can be applied in Information security awareness training and if the benefits of e-learning can be applied in delivering IT Security Awareness.

## 2.5 Conceptual Framework

Following the research conducted, we developed a conceptual framework for the design of the solution that would address some of the gaps that were identified in the current methods of conducting IT Security Awareness. Security awareness in an organization is a learning activity which purposes to increase employees' ability to identify, react to, prevent and report cyber security incidents. It requires involvement from all stakeholders for it to be successful.

The solution will therefore promote a learning activity which will involve all stakeholders from the IT security trainers to the targeted to employees and management by providing different user interfaces for the different roles. The solution will then invoke the cognitive features of employees to be able to drive home the key concepts.

The learning goals and tasks need to be clearly defined from the onset to ensure the program is working towards a defined objective and also to provide a measure which will be used to gauge success of the Security awareness program. The linguistic model used will adopt interaction and dialogue in order to define some abstract IT Security concepts more accurately and their relationships.

One of the main gaps identified was mode of delivery, the developed solution uses several channel types to enhance the modality of the training material we are passing. We have made use of rich multi-media to grab user attention and deliver some of the key messages we want them to take away.

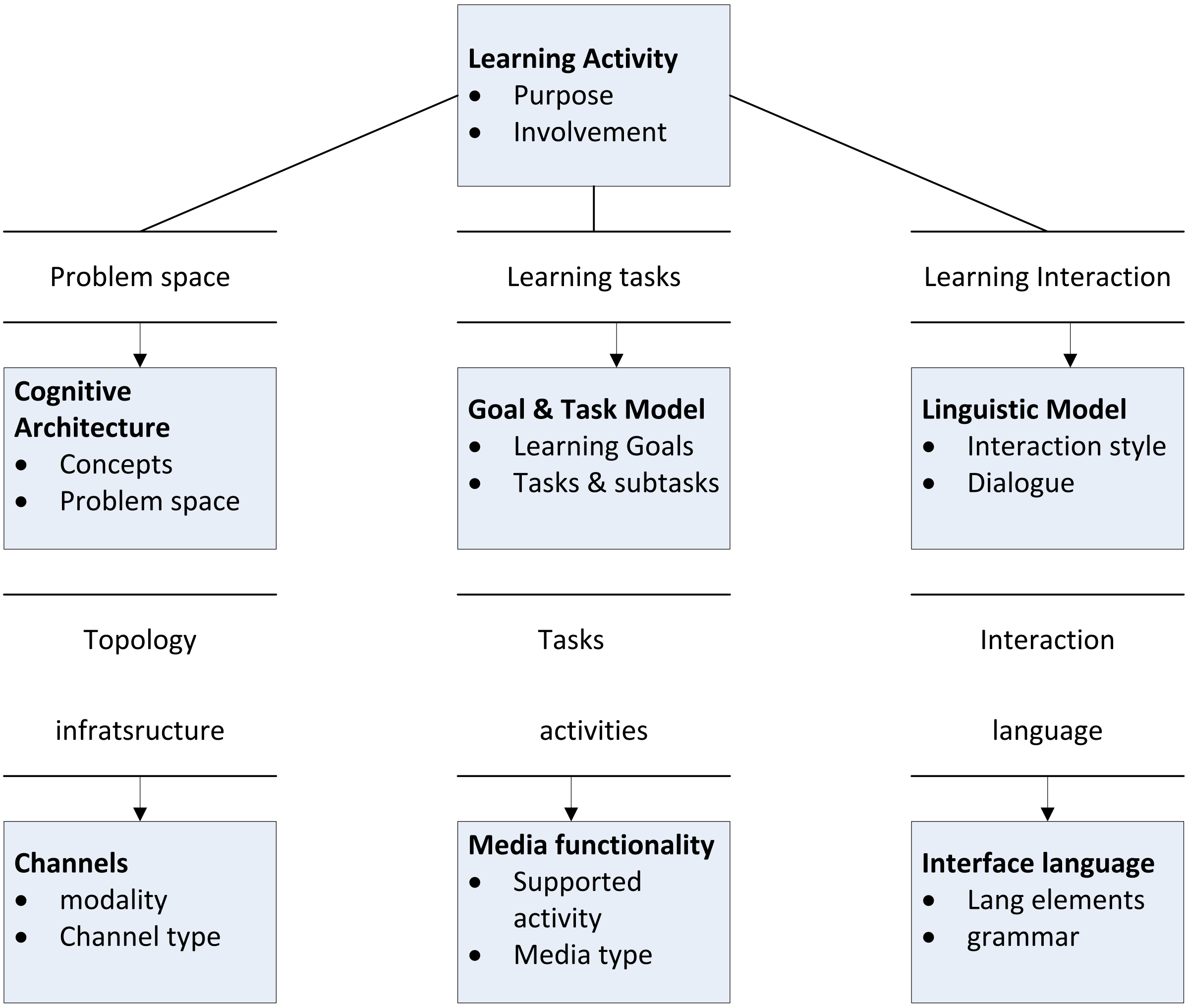


***Figure 2 Conceptual Framework***

# CHAPTER III- METHODOLOGY

In this chapter, we shall discuss the methodology, materials and methods that we used to achieve the research objectives. We have given an account of how the research was carried out by clearly specifying the procedures that were followed in meeting the objectives of the research and the outcome from the different methods used.

In this study, we used Britam Holdings Limited as the primary organization in research and study. It is a large financial services company with presence in seven Pan-African countries whose Head Quarters is in Nairobi Upper-hill. We chose this organization based on the level of maturity of its IT strategy and would use it to give a representation on the deployment of IT Security Awareness programs in financial organizations of similar size and magnitude.

## 3.1 Research Methods

### *3.1.1 Research Design*

In this exploration, we took after a descriptive research design. This sort of design gave answers to the inquiries of who, why and how; connected with our research issue despite the fact that it may not have indisputably discovered answers to why. As we acquired data concerning the ebb and flow status of Security Awareness being used in organizations, descriptive research was exceptionally helpful and helped to portray what existed as factors or conditions in a circumstance.

The research was hypothesis generating. Although the research included finding out the current methods that IT Security awareness is carried out, we were not testing the hypothesis that current Security awareness methods are insufficient but rather generating the hypothesis that Security awareness can be improved using an automated technology supported security awareness program.

### *3.1.2 The Target Population and Sampling Techniques*

This study used Britam Holdings Limited as the primary organization in research and study. It is a large financial services company with presence in seven Pan-African countries whose Head Quarters is in Nairobi Upper-hill. The organization contains around 1000 employees either on permanent, contractual or part-time employees; and salesforce of over 3000 Financial advisors (sales agents) who were not included in the study due to their limited interaction with the organizations Information Systems.

The 100 participants were selected using random sampling which is the purest form of probability sampling. This meant that each member of the population had an equal and known chance of being selected. The selection of 100 participants was a good representative of the entire population size of 1000 hence reducing the margin of error.

The 100 members were chosen using random sampling. This is usually considered among the purest type of probability sampling. This meant that every individual from the population had an equivalent and known chance of being chosen. The choice of 100 participants was a good representation of the whole populace size of 1000 thus diminishing the margin of error.

#### *3.1.2.1 Needs and Assessment*

One of the procedures that can be used to determine an institutions awareness and training needs is doing a needs evaluation. The aftereffects of a requirements evaluation can give defence to persuade management to designate satisfactory assets to meet the distinguished awareness and training needs.

When doing the assessment of needs, the below accompanying key work force were included as part of the target populace.

- Executive Management – Senior Management are very key in any ICT Security initiative. They needed to completely comprehend mandates and laws that frame the reason for the security program. They likewise needed to appreciate their positions of authority in guaranteeing full consistence by employees in their respective units.

- Security Personnel (security program directors and security officers) – These people go about as expert advisors for their organizations and in this way should be knowledgeable on security strategy and approved prescribed procedures.

- System Owners, Administrators and IT Support Personnel – They are responsible for technical expertise over the business support operations and are very key to a fruitful security program, these people required a higher level of specialized learning in compelling security practices and execution.

- Operational Managers and System Users – These group of people required a high level of security awareness and training on security controls and principles of conduct for frameworks they use to direct business operations.

### *3.1.3 Data sources and collection techniques*

To help decide the IT security awareness levels for Britam staff and assist in preparing requirements, an assortment of wellsprings of data was utilized, and there were distinctive approaches to gather that data. These included:

- Surveys sent across the organization
- Discussion with business units' management, data owners, data custodians who support the business systems and application and other association staff whose business capacities depend on IT.
- Review and appraisal of accessible asset material, for example, current awareness and training material, training calendars, and attendance of participants.
- Analysis of measurements identified with awareness and training (e.g., level of clients finishing required awareness).
- Review of security predictions for general supportive networks and significant applications.
- Review of any discoveries as well as suggestions from oversight bodies (Internal audit and contracted external reviews)
- Analysis of occasions, (for example, extent of administrator attacks, site defacing, seizing of frameworks utilized as a part of consequent assaults, fruitful infection assaults etc) demonstrated the requirement for preparing of particular gatherings of individuals.
- Review of when specialized measures or framework changes were made.

Other key methods of data collection like firewall logs, anti-virus reports, user-activity logs and recommendations from oversight bodies provided useful information on the IT Security awareness level of an organization, but could not be published in this study due to the confidential nature of information they reveal.

### *3.1.4 The Instruments*

A great tool that measured the effectiveness and strength of Britam's security awareness program was a survey. The survey design and analysis may seem deceptively simple, merely a process of asking questions and getting answers. But survey research, like any other empirical research, requires careful thought and planning if it is to provide meaningful data and insight.

The three key motivations for selecting a survey were:

1. It offered uniqueness: Information collected may not be available from any other source.
2. Provided a standardized measurement: Systematic collection of data in a structured controlled format.
3. Unbiased representativeness: Selection of sample based on probability distribution.

The design of this employee security awareness survey was influenced by concept, suggestions and examples from SANS securing the human online resources. (SANS, Securing the human, n.d.).

It is an instrument that can provide empirical evidence of security behaviours and attitudes within the organization. The data collected was then used to identify areas of possible improvement and risk reduction. When administered repeatedly over time, the survey would provide a baseline of security awareness that would indicate progress or challenges for the security awareness program.

The survey was administered through an online survey tool, "**Kwiksurveys**" which provided an online platform to deliver the survey, collect results and give an analysis. The survey was anonymous because of asking questions about behaviours that may violate company policy. Respondents were also more likely to be honest if they were not worried that their responses may incriminate them or result in disciplinary measures or victimization.

A copy of the survey has been attached in the appendix.

### *3.1.5 Data collection procedures*

The survey consisted of 26 questions designed to measure a set of basic characteristics of the organization's security awareness posture. Some questions collected factual data (role, location) while others collected data about the user's awareness, attitudes and behaviours. It gathered behavioural data on how users respond to threats, as well as data on attitudes and perceptions of organizational culture. This can help security training and awareness professionals gain a richer, more informed understanding of users' attitudes and habits within the context of their activities.

Response data from this survey was used in several ways, utilizing both qualitative and quantitative analysis techniques. The simplest analysis of the resulting data would be to use descriptive statistical techniques to aggregate responses (number of responses, responses by role, etc.). Such descriptive techniques demonstrated how particular attitudes or behaviours are distributed across the organization.

More advanced quantitative analysis of this data involved using techniques to determine the effectiveness of specific interventions on respondent attitudes and behaviours e.g.  a phishing exercise.

Comparisons across time were accomplished by comparing the descriptive results of this survey. It is important to note that the survey provided visibility into an organization's behaviours, not proof of a certain level of security, awareness or risk. The survey did however allow an organization to measure certain attributes of security awareness that can help tell a story, identify areas of possible concern that should be further explored and support more informed decisions.

### *3.1.6 Processing and analysis*

The review comprised of 26 questions. A portion of the responses in the study showed solid awareness and great security awareness while others demonstrate weak awareness, careless conduct, or high-hazard exercises. In light of these distinctions, each response in this overview (aside from the initial three inquiries) had been allotted a hazard score (1-5). "One" is the least hazard score and "five" is the most noteworthy hazard score. At the point when the aftereffects of the overview had been gathered, they were utilized to decide the general hazard score or hazard level of the organization.

Each exploration question required its own particular investigation, in this manner, the survey questions tended to each one and in turn took after a portrayal of the sort of measurable tests that were to be performed to answer the research question. The inquiries were connected in the reference section itemizing the investigation for each inquiry and the factors that were incorporated into the research. The below examination strategy was recommended by SANS Securing the Human assets. The hazard levels portrayed depended on studies completed by the global body in the course of the last 20 years of information security awareness.

1. *For each of the 26 questions, increase each response hazard score (1-5) by the quantity of times it was picked by the review takers.*

*<response chance value> X <the number of times chosen> = <response total>*

2. *Include the greater part of the response aggregates for a review total reaction summation.*
3. *Divide the overall total response summation by the quantity of review takers to compute the study (or organization's) hazard score.*

*<cumulative reaction total>/<number of overview takers> = Organization's Hazard Score*

4. *Utilizing the hazard score, check the "Hazard Levels" table underneath for the association's general hazard rating.*

***Table 1: Risk Levels***

| Risk | Description |
|---|---|
| Low (25 – 39) | Employees know about great security standards and dangers, have been appropriately prepared, and conform to all authoritative security norms and strategies. |
| Elevated (40 – 60) | Employees have just been prepared on authoritative security guidelines and approaches, they know about dangers, yet may not take after great security standards and controls. |
| Moderate (61 – 81) | Employees know about dangers and know they ought to take after great security standards and controls, however require preparing on hierarchical security norms and arrangements. They additionally may not know how to recognize or report a security occasion. |
| Significant (82 – 96) | Employees don't know about great security standards or dangers nor are they mindful of or agreeable with authoritative security guidelines and arrangements. |
| High (97 – 110) | Employees don't know about dangers and nonchalance known security gauges and approaches or don't consent. They take part in exercises or practices that are effectively assaulted and misused. |

Survey Minimum Risk Score = 25

Survey Maximum Risk Score = 110

### 3.2 Building up a Training and Awareness Strategy and Plan

Gathering and investigation of the Research information enables Britam to build up a procedure for creating, executing, and keeping up its IT security awareness and education strategy. The strategy is the working archive containing the components that make up the system. The strategy ought to talk about the accompanying components:

- Current industry, national and regulations approach that require the training and awareness to be refined and conducted;
- What scope will the information security awareness and training cover;
- Roles and obligations of organization staff who should configure, create, actualize, and keep up the awareness and training material, and who ought to guarantee that the fitting clients go to or see the appropriate material;
- Target groups of participants for every part of the program;
- Mandatory courses or material for each intended interest group;
- Learning goals for every part of the program;
- Topics to be tended to in every session or course;
- Deployment techniques to be utilized for every part of the program;
- Documentation, criticism, and proof of learning for every part of the program;
- Evaluation and refresh of material for every part of the program; and
- Frequency that each intended interest group ought to be presented to material.

## 3.3 Setting up Priorities

Upon conclusion of the security awareness system and plan, we needed to build up a usage plan. In the event that this needed to happen in stages (e.g., because of spending limitations and asset accessibility), it was imperative we choose the elements to be utilized as a part of figuring out which activity to plan first and in what succession. Key variables we considered were:

1. **Availability of Material/Resources**—If awareness and training material and vital assets are promptly accessible, activities in the program can be planned early. In which case, if course material must be produced, trainers must be distinguished and planned, these necessities ought to be considered in setting needs.
2. **Role and Organizational Impact**—It is exceptionally normal to address need as far as authoritative part and hazard. Wide based awareness activities that address the undertaking wide order may get high need in light of the fact that the principles of good security practices can be conveyed to the workforce rapidly. Additionally, it is basic to take a gander at high trust/high effect positions (e.g., IT security program directors, security officers, framework overseers, and security chairmen whose positions in the institution have been resolved to have a higher affectability) and guarantee that they get high need in the rollout system. These sorts of positions are normally equivalent with the kind of access (and to what framework) these clients have.
3. **State of Current Compliance** – This included taking a look at real holes in the awareness and training program and focusing on lacking territories for early rollout.
4. **Critical Project Dependencies** – Ensuring that if there were activities dependent upon a section of security training, keeping in mind the end goal, they were set up and all the essential necessities for the framework included.

## 3.4 System Analysis Design and Development Methods

### *3.4.0 E-Learning Development Methodologies*

The solution adopts the design of e-learning education and structure of instructional learning.

The field of instructional plan and innovation incorporates the investigation of learning and execution issues, and the outline, advancement, usage, assessment and administration of instructional and non-instructional procedures. It makes us of assets and advances planned to enhance learning and execution in an assortment of settings, similar to the work environment.

**Key E-Learning components**

I. **E-learning content**: straightforward learning assets, intelligent e-lessons, electronic recreations.

II. **E-coaching, e-instructing, e-tutoring**: give singular help and input to students through online devices and assistance systems.

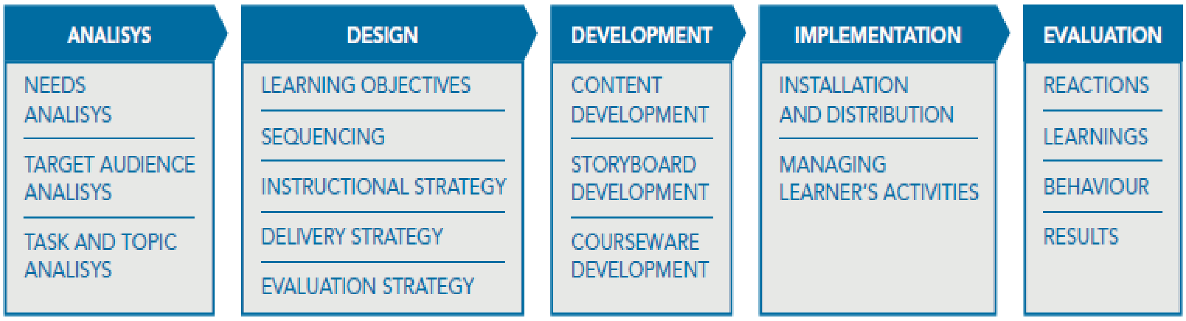
III. **Cooperative, collective learning**: social programming, for example, visits, talk gatherings, intended to encourage correspondence and information sharing among students.

IV. **Virtual classroom**: programming to encourage a teacher to educate remotely and continuously to a gathering of students utilizing a blend of materials

**ADDIE**

This is the classic model that most instructional designers use.

ADDIE stands for Analysis, Design, Development, Implementation and Evaluation.



(FAO, 2011)

***Figure 3: ADDIE***

### *3.4.1 System Analysis and Design*

The project follows the standard Software Development Life Cycle (SDLC) which will be outlined in this section. The activities are highlighted in the diagram below.

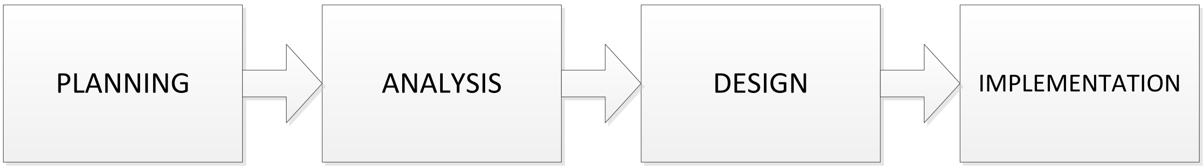


*Figure 4 : Key Activities*

### *3.4.1.1 Planning*

**System request**

| |
|---|
| **Project Sponsor:** Group CIO, IT Security Manager |
| **Business Need:** This project was initiated to reduce Organization risks from cybercrime by increasing awareness levels of staff. The system provided an online method for delivering IT Security awareness to the group. This enabled faster, cost effective, widespread, interactive and customized training to cover the wide reach of the company. And the material was made available online when required by staff. |
| **Business Requirements:** Using the System, the IT Security Team will be able to deliver awareness across the entire group in all in scope countries with reduced effort and fatigue and fewer costs from travelling. It enables management track who is compliant to the training and will make material available to all staff on an online platform. Specific Requirements are:<br>• Online Training Material<br>• Customized content for different business units and countries<br>• Tracking of training attendance for management<br>• Metrics for tracking impact of training<br>• Online assessment<br>• Reporting for management and compliance |
| **Business Value:**<br>• Increased awareness level reducing organizational exposure to online fraud and cyber crimes<br>• Enable IT Security team to focus efforts on key strategic tasks by reducing time spend on travel to deliver awareness physically across entire company reach.<br>• Reduce costs of travel and accommodation spent by IT staff when travelling across Kenya and other countries to carry out awareness<br>• Compliance to regulatory authorities on requirements for mandatory awareness trainings. |

### *3.4.1.2 Analysis*

This stage was very critical to the success of the solution. The evaluation done in this stage enabled us identify who will utilize the solution. It helped clearly highlight what the system will do, and also where and when it will be utilized. Amid this stage, we examined the present framework, distinguished change openings, and build up an idea for the new framework that we used for the solution.

### Analysis Strategy

The analysis phase involved understanding the as-is situation. The as is situation was helpful in understanding what improvements need to be made in the new system so that we could gather requirements for the new system. In the current situation, there was no system being used to carry out Security awareness training as has been discussed through most of this paper, we therefore identified that one of our objectives was to automate the current processes so we can move from "where we were" to "where we wanted to be".

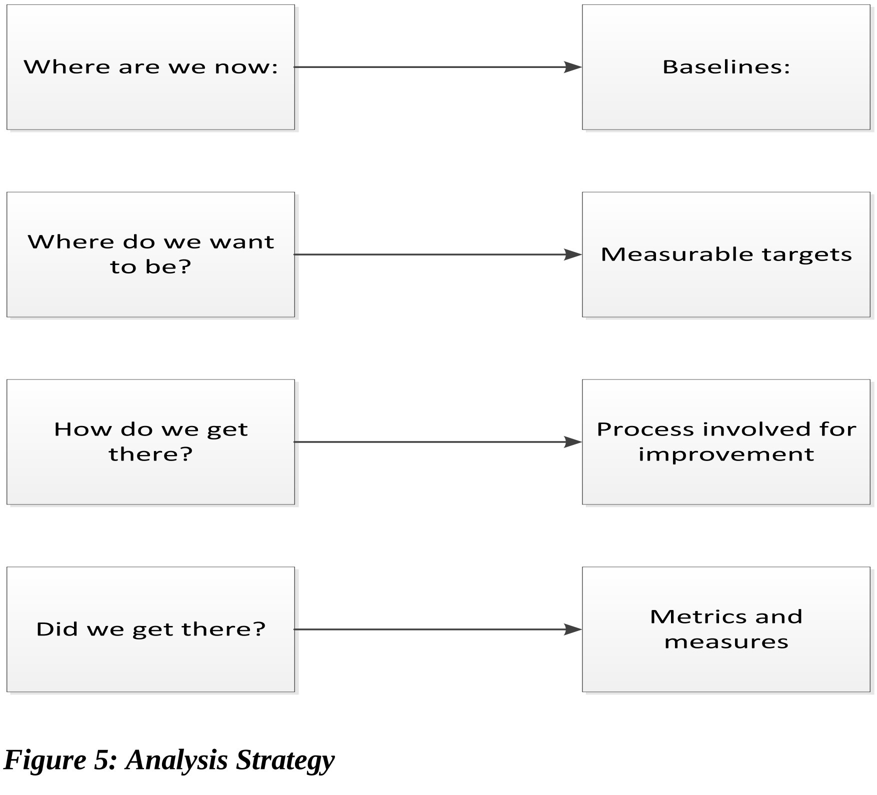


***Figure 5: Analysis Strategy***

Currently as highlighted in the background statement and introduction of my study, there was no system being used to carry out or aid the Security awareness training. This had been working so far, but with its share of challenges as highlighted in the problem statement and literature review. These included:

- Insufficient Delivery methods
- security awareness material content generalization
- Lack of metrics for tracking deployment
- Lack of metrics for measuring impact of Security awareness training

Improvements were made by providing a solution which would addresses some if not all of the above shortcomings. Analysis of the above shortcomings and also data collected from interaction and interviewing some of the major stakeholders was helpful towards determining the user’s requirements, functional requirements and system requirements.

### Requirements Definition

The next phase in the analysis phase focused on the requirements determination. This had several categories including: Business, functional, non-functional and technology requirements.

### Business Requirements

To be able to add value to the business the system should be able to meet the following requirements:

1. The system should be able to simulate attacks through email as this is the primary point of entry for cyberattacks.
2. The system should be able to provide the Security awareness material online such that it can be available to employees authorized to access it.
3. The system will be able to track the attendance and completion of security awareness training for management purposes and compliance.
4. The system will be able to measure the risk levels of the organization, identify the highest risk employees or business functions.
5. The system will be able to measure impact of the training and show whether employees and employee behaviour is improving.
6. The system should be able to provide interactive delivery means including simulations, interactive learning content to supplement the classroom awareness training.

The critical analysis of the above business requirements informed the functional requirements which the system should meet. For the system to meet those requirements it required to have the below functional requirements.

### Functional Requirements

1. Send email functionality to be able to forward simulated attacks.
2. Simulate attacks and capture details of responses to attacks.
3. The system will be a web application hosted on a webserver with the below functions:
    - It will allow administrators to enrol trainers and trainees.
    - The trainers can upload and prepare learning content
    - Trainers can enrol trainees for courses
    - Students can self-enrol on courses enabled for self-enrolment.
4. The system must be able to track progress of training, show completion status for courses enrolled for, report on training status for a particular course
5. The system shall be able to measure the awareness level of individuals by using simulations to show high risk employees who fall victim of simulated attacks.
6. The system should be able to compare and analyse employees' performance on: (quizzes and tests, simulated attacks) to determine whether employee is improving.
7. The system should allow for uploading of multimedia content accessible via flash and html.
8. The system should be able to send out simulated attacks and analyse results from the tests.

### Non-Functional Requirements

#### a. Operational

- The system should run on PCs and tablets with a web browser.
- The system should support mail functionality by linking to a SMTP server.
- The system can be linked to an LDAP directory for user enrolment and importing.

#### b. Performance

- The system should support total 100 concurrent users
- Limit media size of multimedia content to be uploaded.
- The System should have a throughput of 100emails per day.

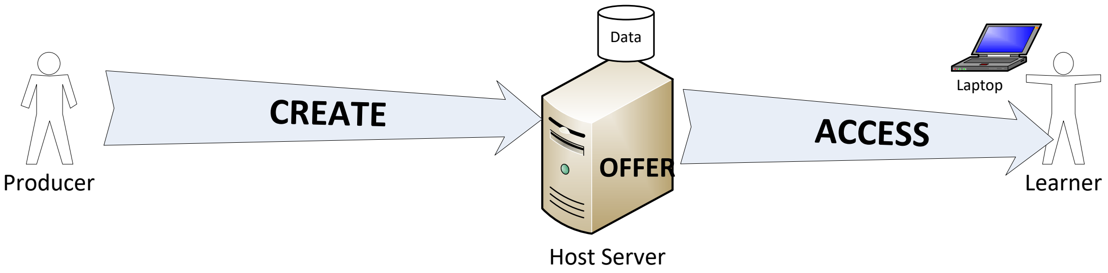
#### c. Security

- The system will be secured through SSL to enable secure communications.
- Access will be managed to ensure only authorized personnel can access system.
- Role based access control to prevent normal users having access to what they are not authorized.
- Courses can only be deleted by the administrators upon managerial approval.

**d. Cultural and Legal**

- Personally identifiable information (PII) must be protected as stated in Data Privacy and protection Acts
- The system will confirm to internal ICT security policies

## Technology Requirements



| | | | |
|---|---|---|---|
| Hardware | Multimedia workstation | Network Server | Personal Computer |
| Connection | Moderate Speed | High Speed | Moderate Speed |
| Software | Authoring Software | Webserver software | Browser and Media players |

***Figure 6: Technology requirements by participants***

## Use Case

From the above critical analysis, we are able to capture the requirements specifications. The specifications guided the shape and structure of the proposed system and how the users interacted with the system.

We utilized the below case situations to portray how the system associated with its condition by delineating the exercises that were performed by the clients of the solution and the system's reactions.

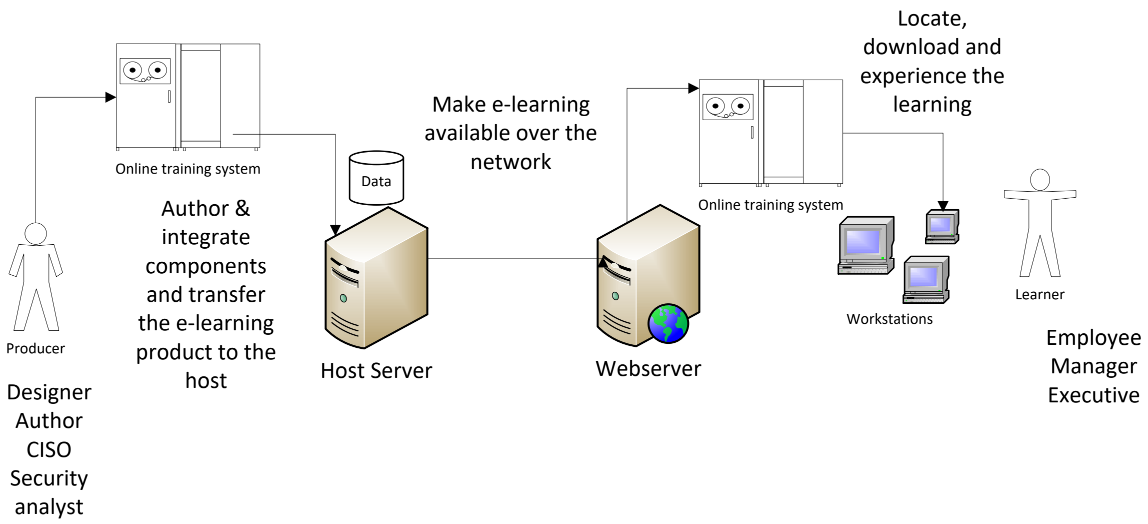


*Figure 7: High level use case scenario*

**Producers** include the designers, authors, writers, illustrators who collaboratively gather e-learning products into reality.

**Learners** can be referred to in many ways. They are the employees targeted by the online security awareness training.

**The host** is the ICT Infrastructure that facilitates e-learning to be generally accessible over a network. It makes the learning item available to intended learners and the individuals who must oversee, keep up, facilitate and bolster it.

The **Online training system** is the proposed system that will be used to deliver online security awareness training. The proposed system has been broken down as below based on the interactions and processes with the actors on the system.

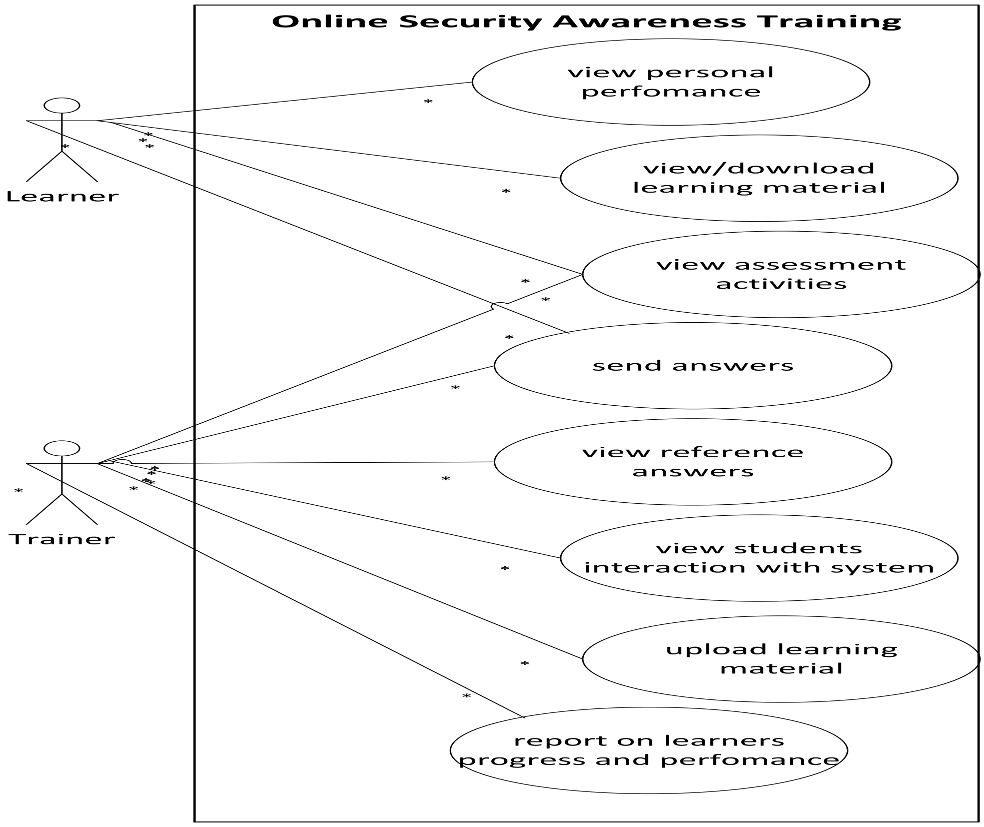

Online Security Awareness Training
view personal perfomance
view/download learning material
view assessment activities
send answers
view reference answers
view students interaction with system
upload learning material
report on learners progress and perfomance
Learner
Trainer
*

***Figure 8: Detailed use case for trainer and trainee roles***

Learners are the trainees receiving the security awareness training. They can:

- Access online learning material
- Carry out self-assessment activities
- Send answers to quizzes/tests set by the trainers
- View the progress of their training and results of assessments

The trainers are the users who are added to facilitate training through the system. They can:

- Upload learning content
- View responses to assessments submitted by learners
- View learners' interaction with the system
- Create assessments for the learners
- Run reports on learning progress of the learners and performance

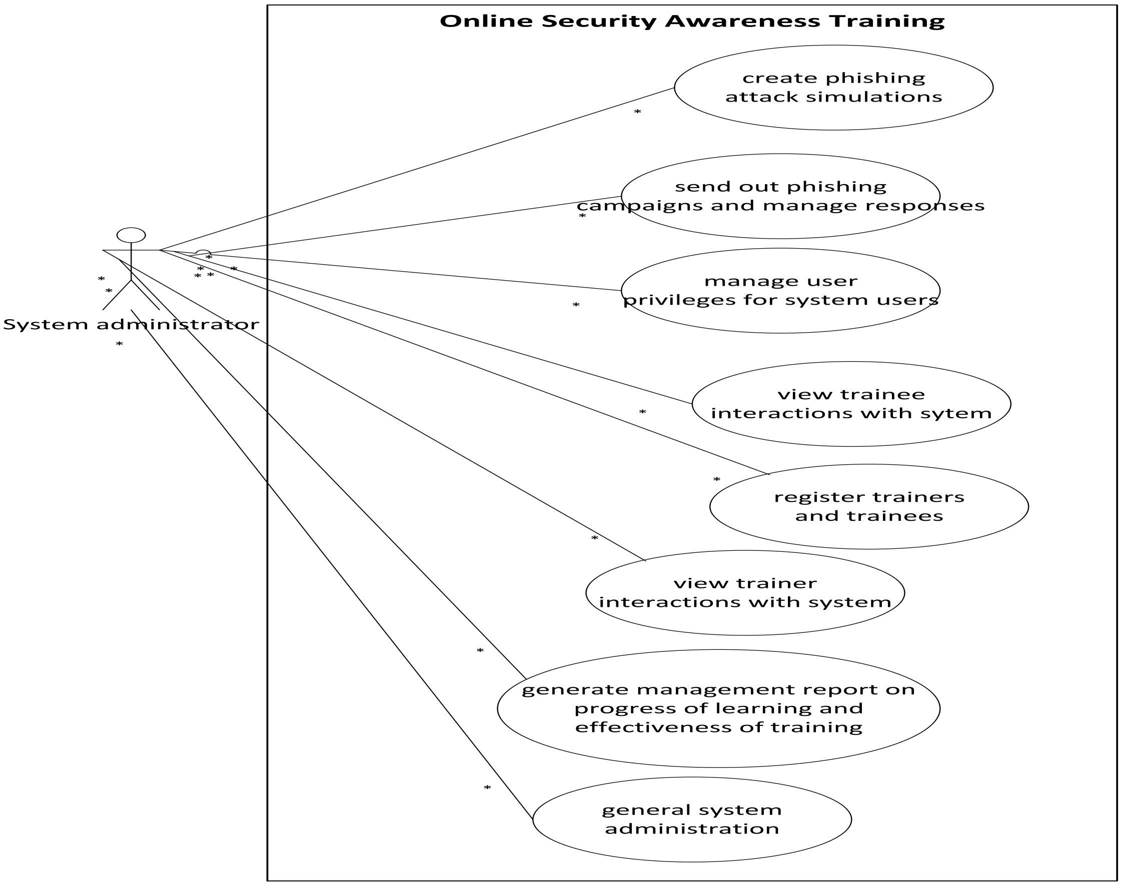

Online Security Awareness Training
create phishing attack simulations
send out phishing campaigns and manage responses
manage user privileges for system users
view trainee interactions with sytem
register trainers and trainees
view trainer interactions with system
generate management report on progress of learning and effectiveness of training
general system administration
System administrator
*

***Figure 9: Detailed use case scenario for System administrator***

The system administration will be tasked with primarily managing the system, this includes:

- Creation simulated attacks
- Launch and track response to simulated attacks.
- Managing the learners and trainers,
- Ensure only authorized users can access the system and ensure access rights are assigned to the right role.
- Manage trainer interactions with system.
- Manage trainee interactions with system.
- Manage learning content.
- Backup system.
- Reporting on training progress and effectiveness of training.

- Activate and deactivate courses
- Update system functionality

### 3.4.1.1 Design

For us to determine how the system would operate, in terms of software applications, network infrastructure and the hardware integrations', we needed to carry out the design stage. This enabled us outline and design our forms, user interfaces, reports that were used. It also enabled us to blue print and model the databases, specific programs and software development models that were required.

### Class Diagram

Class diagrams are the backbone of object-oriented programming and software design. Class diagrams demonstrate the classes of systems,they describe the attributes and operations of a class, how they interrelate and the constraints that are imposed on the system.. Class charts are utilized for a wide assortment of purposes, including both theoretical/area demonstrating and point by point configuration modelling, (Rumbaugh, 1991) . The below class diagram shows the functions of the online Phishing simulator which was used to simulate attacks and deliver edcation and awareness to users.

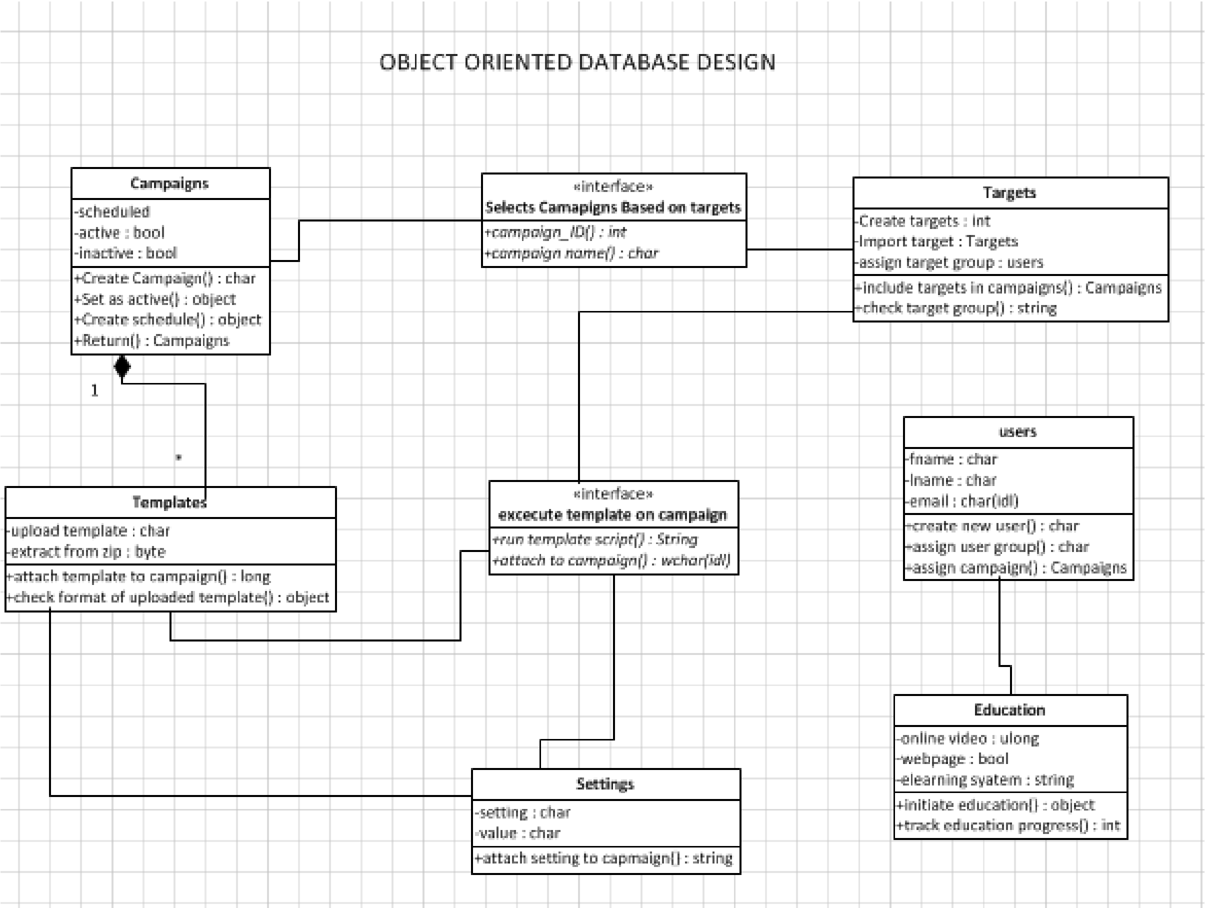
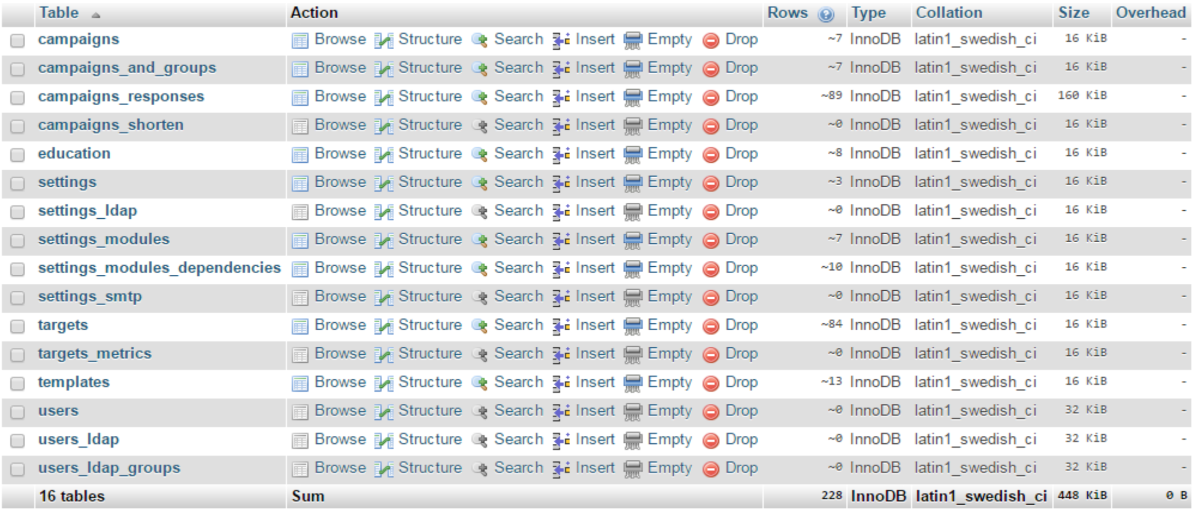

OBJECT ORIENTED DATABASE DESIGN
Campaigns
-scheduled
-active : bool
-inactive : bool
+Create Campaign() : char
+Set as active() : object
+Create schedule() : object
+Return() : Campaigns
1
*
«interface»
Selects Camapigns Based on targets
+campaign_ID() : int
+campaign name() : char
Targets
-Create targets : int
-Import target : Targets
-assign target group : users
+include targets in campaigns() : Campaigns
+check target group() : string
users
-fname : char
-lname : char
-email : char(idl)
+create new user() : char
+assign user group() : char
+assign campaign() : Campaigns
Templates
-upload template : char
-extract from zip : byte
+attach template to campaign() : long
+check format of uploaded template() : object
«interface»
excecute template on campaign
+run template script() : String
+attach to campaign() : wchar(idl)
Education
-online video : ulong
-webpage : bool
-elearning syatem : string
+initiate education() : object
+track education progress() : int
Settings
-setting : char
-value : char
+attach setting to capmaign() : string

*Figure 10: Class Diagram*

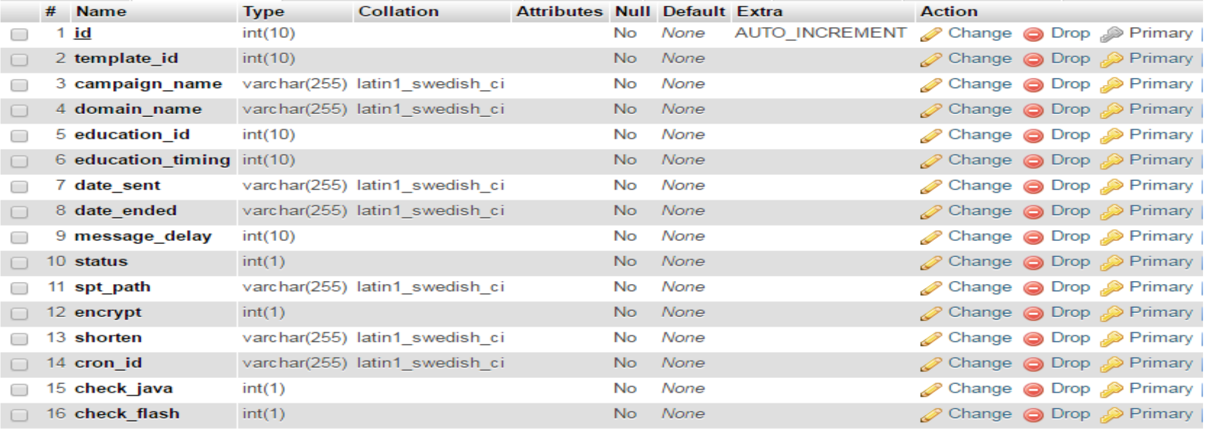
## Data Dictionary

The gathering of depiction of data objects, tables, descriptions or articles in a database for the advantage of software engineers, system analysts and designers is referred to as a data dictionary. The information contained list the tables in the database and their structure and demonstrates all the conceivable perspectives and operations the database could perform.



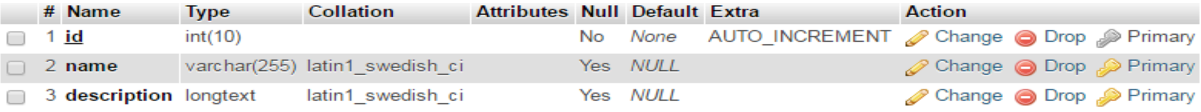
| | Table | Action | Rows | Type | Collation | Size | Overhead |
|---|---|---|---|---|---|---|---|
| □ | campaigns | Browse Structure Search Insert Empty Drop | ~7 | InnoDB | latin1_swedish_ci | 16 KiB | - |
| □ | campaigns_and_groups | Browse Structure Search Insert Empty Drop | ~7 | InnoDB | latin1_swedish_ci | 16 KiB | - |
| □ | campaigns_responses | Browse Structure Search Insert Empty Drop | ~89 | InnoDB | latin1_swedish_ci | 160 KiB | - |
| □ | campaigns_shorten | Browse Structure Search Insert Empty Drop | ~0 | InnoDB | latin1_swedish_ci | 16 KiB | - |
| □ | education | Browse Structure Search Insert Empty Drop | ~8 | InnoDB | latin1_swedish_ci | 16 KiB | - |
| □ | settings | Browse Structure Search Insert Empty Drop | ~3 | InnoDB | latin1_swedish_ci | 16 KiB | - |
| □ | settings_ldap | Browse Structure Search Insert Empty Drop | ~0 | InnoDB | latin1_swedish_ci | 16 KiB | - |
| □ | settings_modules | Browse Structure Search Insert Empty Drop | ~7 | InnoDB | latin1_swedish_ci | 16 KiB | - |
| □ | settings_modules_dependencies | Browse Structure Search Insert Empty Drop | ~10 | InnoDB | latin1_swedish_ci | 16 KiB | - |
| □ | settings_smtp | Browse Structure Search Insert Empty Drop | ~0 | InnoDB | latin1_swedish_ci | 16 KiB | - |
| □ | targets | Browse Structure Search Insert Empty Drop | ~84 | InnoDB | latin1_swedish_ci | 16 KiB | - |
| □ | targets_metrics | Browse Structure Search Insert Empty Drop | ~0 | InnoDB | latin1_swedish_ci | 16 KiB | - |
| □ | templates | Browse Structure Search Insert Empty Drop | ~13 | InnoDB | latin1_swedish_ci | 16 KiB | - |
| □ | users | Browse Structure Search Insert Empty Drop | ~0 | InnoDB | latin1_swedish_ci | 32 KiB | - |
| □ | users_ldap | Browse Structure Search Insert Empty Drop | ~0 | InnoDB | latin1_swedish_ci | 32 KiB | - |
| □ | users_ldap_groups | Browse Structure Search Insert Empty Drop | ~0 | InnoDB | latin1_swedish_ci | 32 KiB | - |
| | 16 tables | Sum | 228 | InnoDB | latin1_swedish_ci | 448 KiB | 0 B |

*Figure 11: Database structure*



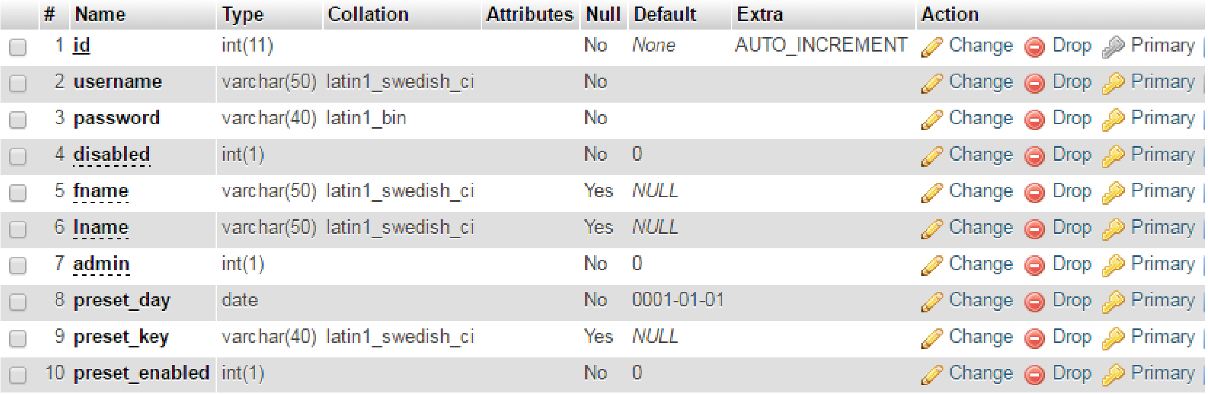
| | # | Name | Type | Collation | Attributes | Null | Default | Extra | Action |
|---|---|---|---|---|---|---|---|---|---|
| □ | 1 | id | int(10) | | | No | *None* | AUTO_INCREMENT | Change Drop Primary |
| □ | 2 | template_id | int(10) | | | No | *None* | | Change Drop Primary |
| □ | 3 | campaign_name | varchar(255) | latin1_swedish_ci | | No | *None* | | Change Drop Primary |
| □ | 4 | domain_name | varchar(255) | latin1_swedish_ci | | No | *None* | | Change Drop Primary |
| □ | 5 | education_id | int(10) | | | No | *None* | | Change Drop Primary |
| □ | 6 | education_timing | int(10) | | | No | *None* | | Change Drop Primary |
| □ | 7 | date_sent | varchar(255) | latin1_swedish_ci | | No | *None* | | Change Drop Primary |
| □ | 8 | date_ended | varchar(255) | latin1_swedish_ci | | No | *None* | | Change Drop Primary |
| □ | 9 | message_delay | int(10) | | | No | *None* | | Change Drop Primary |
| □ | 10 | status | int(1) | | | No | *None* | | Change Drop Primary |
| □ | 11 | spt_path | varchar(255) | latin1_swedish_ci | | No | *None* | | Change Drop Primary |
| □ | 12 | encrypt | int(1) | | | No | *None* | | Change Drop Primary |
| □ | 13 | shorten | varchar(255) | latin1_swedish_ci | | No | *None* | | Change Drop Primary |
| □ | 14 | cron_id | varchar(255) | latin1_swedish_ci | | No | *None* | | Change Drop Primary |
| □ | 15 | check_java | int(1) | | | No | *None* | | Change Drop Primary |
| □ | 16 | check_flash | int(1) | | | No | *None* | | Change Drop Primary |

*Figure 12: Campaigns Table*



| | # | Name | Type | Collation | Attributes | Null | Default | Extra | Action |
|---|---|---|---|---|---|---|---|---|---|
| □ | 1 | id | int(10) | | | No | *None* | AUTO_INCREMENT | Change Drop Primary |
| □ | 2 | name | varchar(255) | latin1_swedish_ci | | Yes | *NULL* | | Change Drop Primary |
| □ | 3 | description | longtext | latin1_swedish_ci | | Yes | *NULL* | | Change Drop Primary |

*Figure 13: Education Table*



|  | # | Name | Type | Collation | Attributes | Null | Default | Extra | Action |
|---|---|---|---|---|---|---|---|---|---|
| ☐ | 1 | id | int(11) |  |  | No | *None* | AUTO_INCREMENT | Change Drop Primary \| |
| ☐ | 2 | **username** | varchar(50) | latin1_swedish_ci |  | No |  |  | Change Drop Primary \| |
| ☐ | 3 | **password** | varchar(40) | latin1_bin |  | No |  |  | Change Drop Primary \| |
| ☐ | 4 | **disabled** | int(1) |  |  | No | 0 |  | Change Drop Primary \| |
| ☐ | 5 | **fname** | varchar(50) | latin1_swedish_ci |  | Yes | *NULL* |  | Change Drop Primary \| |
| ☐ | 6 | **lname** | varchar(50) | latin1_swedish_ci |  | Yes | *NULL* |  | Change Drop Primary \| |
| ☐ | 7 | **admin** | int(1) |  |  | No | 0 |  | Change Drop Primary \| |
| ☐ | 8 | **preset_day** | date |  |  | No | 0001-01-01 |  | Change Drop Primary \| |
| ☐ | 9 | **preset_key** | varchar(40) | latin1_swedish_ci |  | Yes | *NULL* |  | Change Drop Primary \| |
| ☐ | 10 | **preset_enabled** | int(1) |  |  | No | 0 |  | Change Drop Primary \| |

***Figure 14: Users Table***

### 3.4.1.2 Development and Implementation

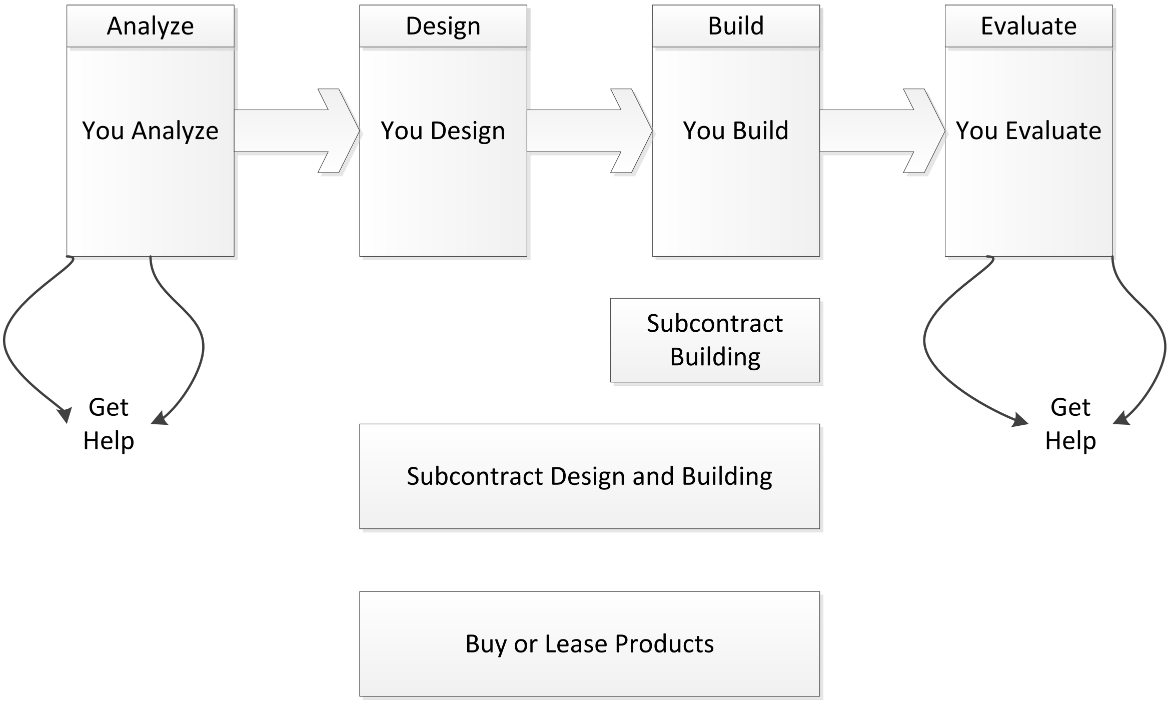


***Figure 15 : E-learning Software Development Process***

Creating learning items is an intricate and costly process. One does not necessarily have to manage and handle each and every one of these issues. A wise approach is to subcontract a portion of the work. You may be able to get a third-party to manage some similar devices, innovations and services that are required. All that you need to ensure is that you comprehend the fundamental specialized abilities required without need to buy, Implement, maintain, and administer the devices.

Although the entire developmental cycle could be subcontracted, it is common to have some phases that are more outsourced than others. For this particular project, based on time constraints, we developed part of the system while the other parts were outsourced as software as a service.

**Web Based Technologies**

When developing web applications, we utilize a vast majority of online based innovations, scripting languages, technologies and platforms. Due to the enhancement in technology, most of them are open-source free and meet the globally accepted standards of (W3C). The ones that we utilized were:

- **HTML, XHTML, CSS**

You cannot build websites without the knowledge of HTML. HyperText Markup Language (HTML) is the standard markup dialect for making web pages and web applications. It allows one to organize their images, text and videos on a web pages.

Cascading Style Sheets (CSS) on the other hand describe how HTML documents should be styled and displayed. These provide the look and feel of our web application making the interface more appealing.

- **PHP server scripting language**

PHP (Hypertext Preprocessor), is a server-side scripting dialect. It is a well-known open source HTML-installed scripting dialect, which is upheld by many Web servers including Apache hypertext exchange convention (HTTP) Server and is the favoured Linux Web scripting dialect. It allowed us to design and compose powerfully and create dynamic pages rapidly.

- **Extensible Mark-up language (XML)**

XML- Extensible Markup Language. XML is a markup dialect fundamentally the same as and identified with HTML, however HTML is utilized to increase content for introduction purposes while XML is utilized to increase content for information portrayal purposes (Evjen et al., 2007). XML was intended to portray information. XML labels are not pre characterized you should characterize your own labels.

It defines a set of rules that are used to encode documents into a format that is readable by both machine and human.

- **MySQL WAMP server for hosting and providing a web-server**

WampServer is a utility that permits you to develop Web applications and oversee your server and databases. It comes with utilities which provide interfaces for conducting numerous server administration tasks.

This may include creating databases, modifying table structures, setting user access privileges, viewing and modifying the server configuration, and querying table data (Gilmore, 2004).

The *"phpMyAdmin"* is another MySQL client. It is a Web-based, third-party client tool which is very powerful in managing MySQL databases developed in PHP. It is known to popularly offer a number of compelling features and is very stable. (Gilmore, 2004):

- Being browser-based, it provides convenient and easy administration of remote MySQL databases from the simple click of a browser.
- Admin can practice full control over client benefits, passwords and asset utilization, and in addition make, erase and even duplicate client accounts

**Sharable Content Object Reference Model (SCORM)**

The online learning system stuck to standards and the Sharable Content Object Reference Model (SCORM) was the standard to be adopted. The online solution was SCORM-compliant learning system so as to properly deliver and track SCORM-compliant learning content.

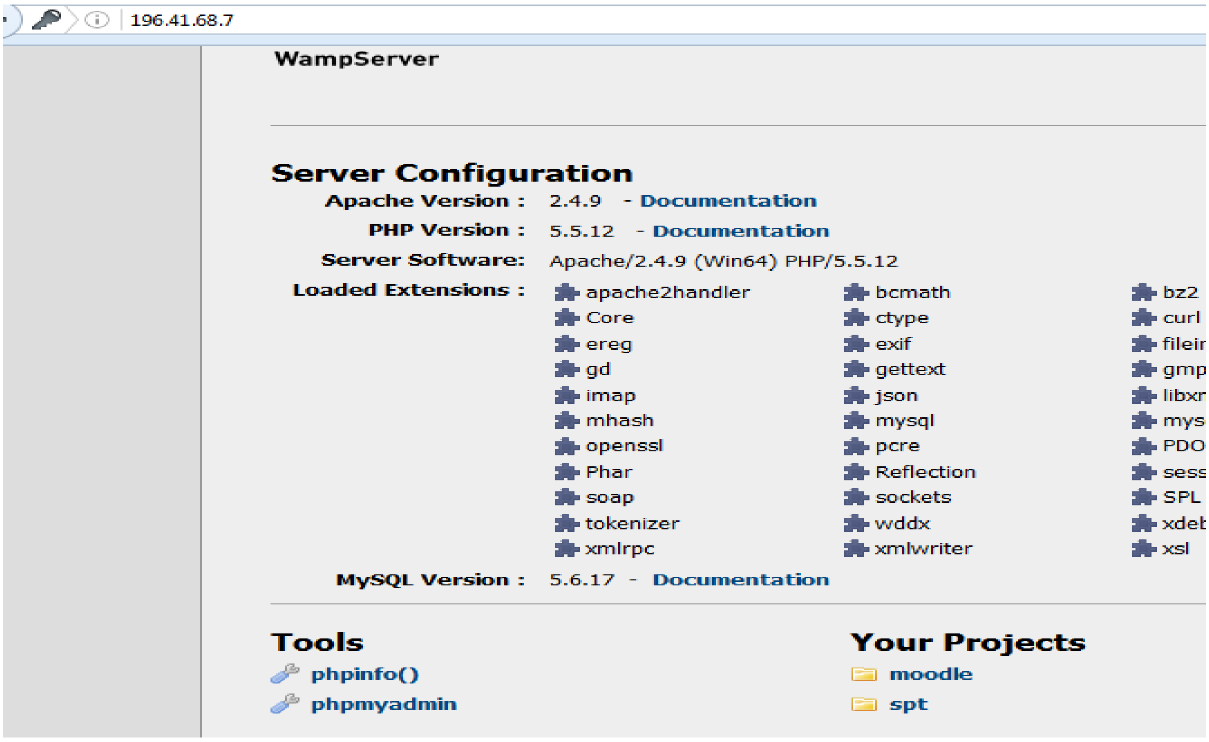
SCORM is a suite of technical standards that enable Web-based learning systems to find, import, share, reuse, and export learning content in a standardized way. The SCORM is a conceptual model describing how to manage, package and deliver learning information so that it can be easily shared on the Internet. The eLearning solution used for this scenario ran as software as a service outsourced to be able to deliver content in SCORM compliant manner.

Being a web based learning framework, it was ideal to stick to norms and guidelines of which Sharable Content Object Reference Model (SCORM) is the standard to be received. The online training is a SCORM-consistent learning framework in order to legitimately convey and track SCORM-agreeable learning content.

SCORM is a suite of specialized benchmarks that empower Web-based learning frameworks to find, import, share, reuse, and send out learning material in a consistent manner. The SCORM is a calculated model that portrays how one should bundle, oversee and convey learning data with the goal that it can be effectively shared on the Internet. The model of eLearning arrangement that was utilized for the purposes of this research was implemented as software as service outsourced to have the capacity to convey content in SCORM consistent way.

**Developing the online attack simulation application**

The tool was developed in PHP as the web scripting language; it was set-up on a local server with WAMP installed to act as the webserver for Apache and Tomcat services and provide phpMyAdmin for administering the database. The server was setup on host: 196.41.68.7, this is a NATTED IP to prevent disclosure of the internal private IP address.



196.41.68.7

WampServer

**Server Configuration**

Apache Version : 2.4.9 - Documentation

PHP Version : 5.5.12 - Documentation

Server Software: Apache/2.4.9 (Win64) PHP/5.5.12

Loaded Extensions :

apache2handler, Core, ereg, gd, imap, mhash, openssl, Phar, soap, tokenizer, xmlrpc

bcmath, ctype, exif, gettext, json, mysql, pcre, Reflection, sockets, wddx, xmlwriter

bz2, curl, fileir, gmp, libxr, mys, PDO, sess, SPL, xdeb, xsl

MySQL Version : 5.6.17 - Documentation

**Tools**

phpinfo()

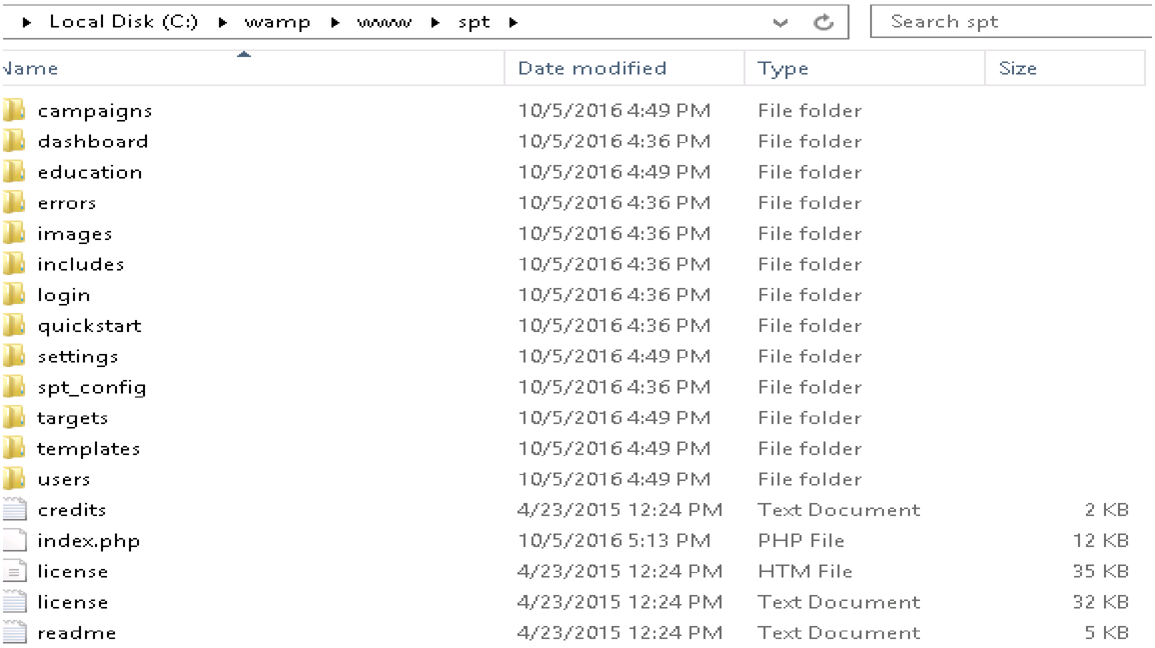
phpmyadmin

**Your Projects**

moodle

spt

*Figure 16: Host Server*

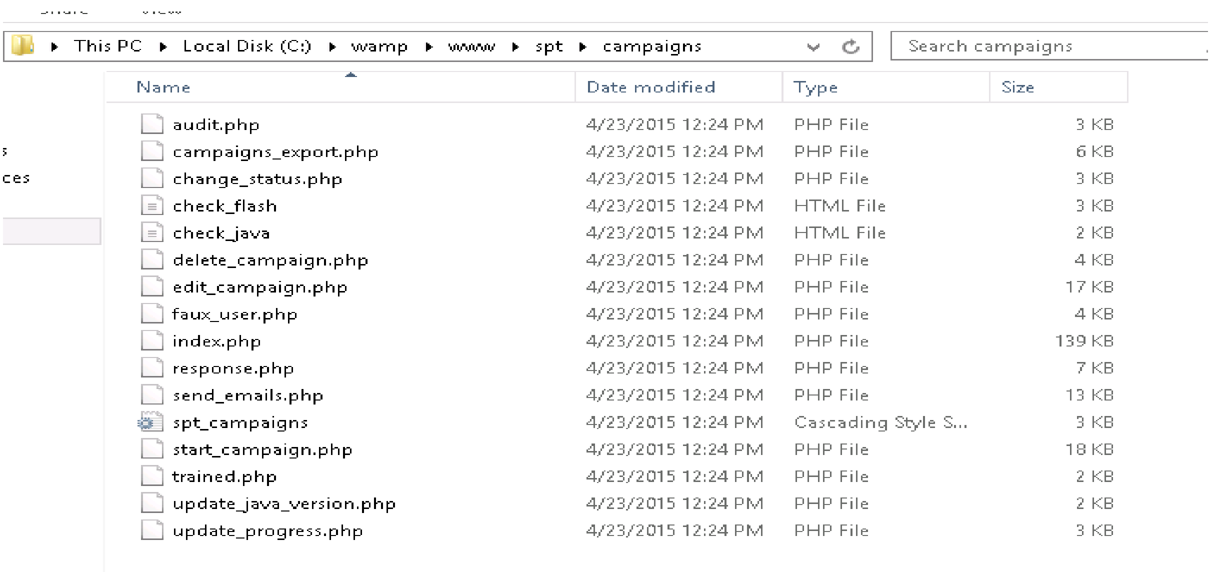


▸ Local Disk (C:) ▸ wamp ▸ www ▸ spt ▸

Search spt

| Name | Date modified | Type | Size |
|---|---|---|---|
| campaigns | 10/5/2016 4:49 PM | File folder | |
| dashboard | 10/5/2016 4:36 PM | File folder | |
| education | 10/5/2016 4:49 PM | File folder | |
| errors | 10/5/2016 4:36 PM | File folder | |
| images | 10/5/2016 4:36 PM | File folder | |
| includes | 10/5/2016 4:36 PM | File folder | |
| login | 10/5/2016 4:36 PM | File folder | |
| quickstart | 10/5/2016 4:36 PM | File folder | |
| settings | 10/5/2016 4:49 PM | File folder | |
| spt_config | 10/5/2016 4:36 PM | File folder | |
| targets | 10/5/2016 4:49 PM | File folder | |
| templates | 10/5/2016 4:49 PM | File folder | |
| users | 10/5/2016 4:49 PM | File folder | |
| credits | 4/23/2015 12:24 PM | Text Document | 2 KB |
| index.php | 10/5/2016 5:13 PM | PHP File | 12 KB |
| license | 4/23/2015 12:24 PM | HTM File | 35 KB |
| license | 4/23/2015 12:24 PM | Text Document | 32 KB |
| readme | 4/23/2015 12:24 PM | Text Document | 5 KB |

***Figure 17: Root directory***



▸ This PC ▸ Local Disk (C:) ▸ wamp ▸ www ▸ spt ▸ campaigns

Search campaigns

| Name | Date modified | Type | Size |
|---|---|---|---|
| audit.php | 4/23/2015 12:24 PM | PHP File | 3 KB |
| campaigns_export.php | 4/23/2015 12:24 PM | PHP File | 6 KB |
| change_status.php | 4/23/2015 12:24 PM | PHP File | 3 KB |
| check_flash | 4/23/2015 12:24 PM | HTML File | 3 KB |
| check_java | 4/23/2015 12:24 PM | HTML File | 2 KB |
| delete_campaign.php | 4/23/2015 12:24 PM | PHP File | 4 KB |
| edit_campaign.php | 4/23/2015 12:24 PM | PHP File | 17 KB |
| faux_user.php | 4/23/2015 12:24 PM | PHP File | 4 KB |
| index.php | 4/23/2015 12:24 PM | PHP File | 139 KB |
| response.php | 4/23/2015 12:24 PM | PHP File | 7 KB |
| send_emails.php | 4/23/2015 12:24 PM | PHP File | 13 KB |
| spt_campaigns | 4/23/2015 12:24 PM | Cascading Style S... | 3 KB |
| start_campaign.php | 4/23/2015 12:24 PM | PHP File | 18 KB |
| trained.php | 4/23/2015 12:24 PM | PHP File | 2 KB |
| update_java_version.php | 4/23/2015 12:24 PM | PHP File | 2 KB |
| update_progress.php | 4/23/2015 12:24 PM | PHP File | 3 KB |

***Figure 18: Campaigns Directory***

The scripts were edited on notepad++ for creating different functionality in the system, the source was compiled, run and the system backend accessed through a browser interface. The initial login page is as below.

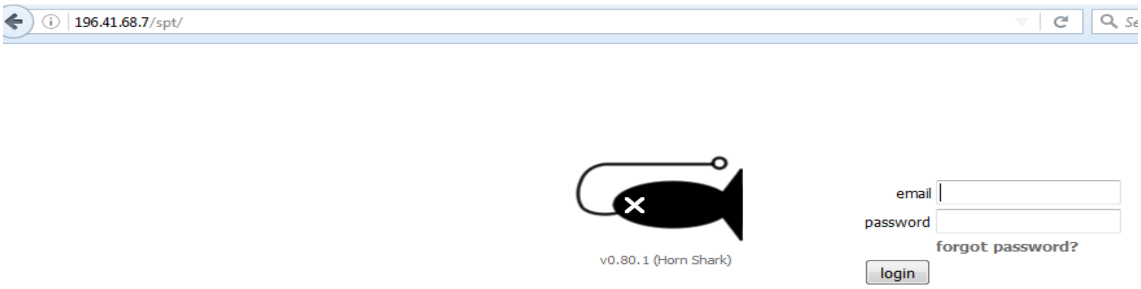
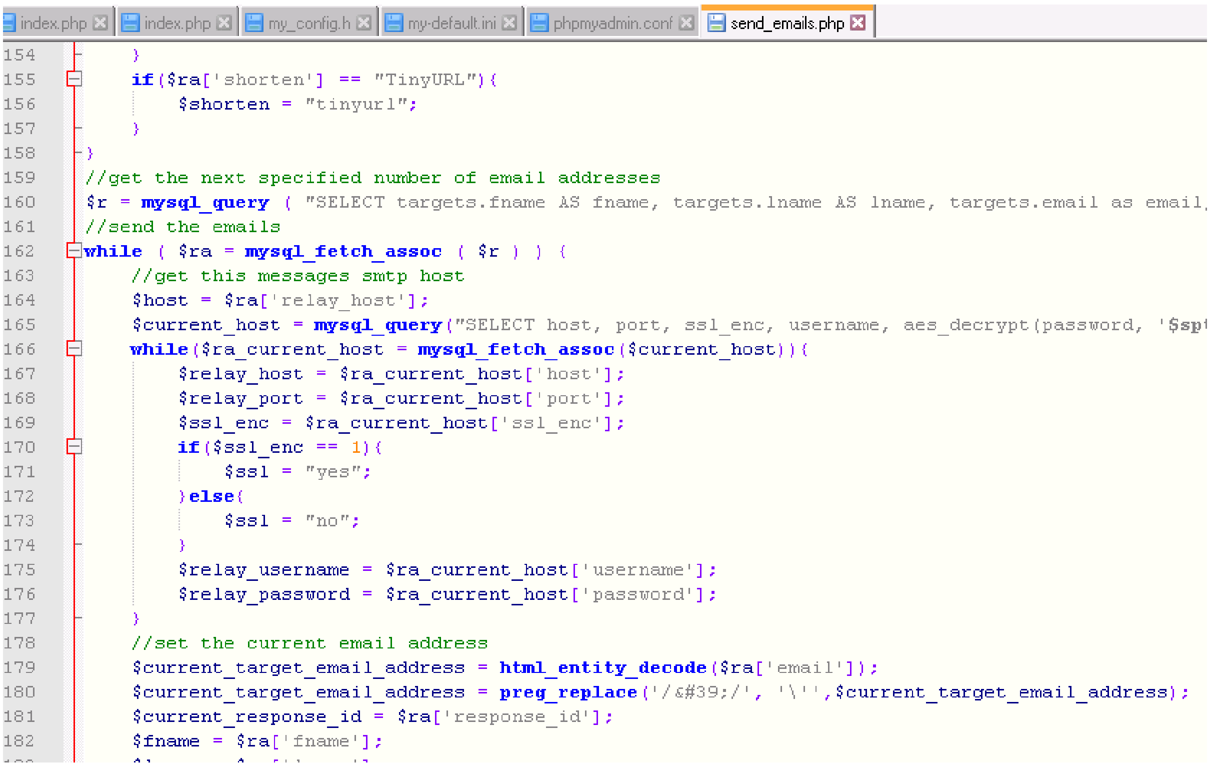


*Figure 19: Log in screen*

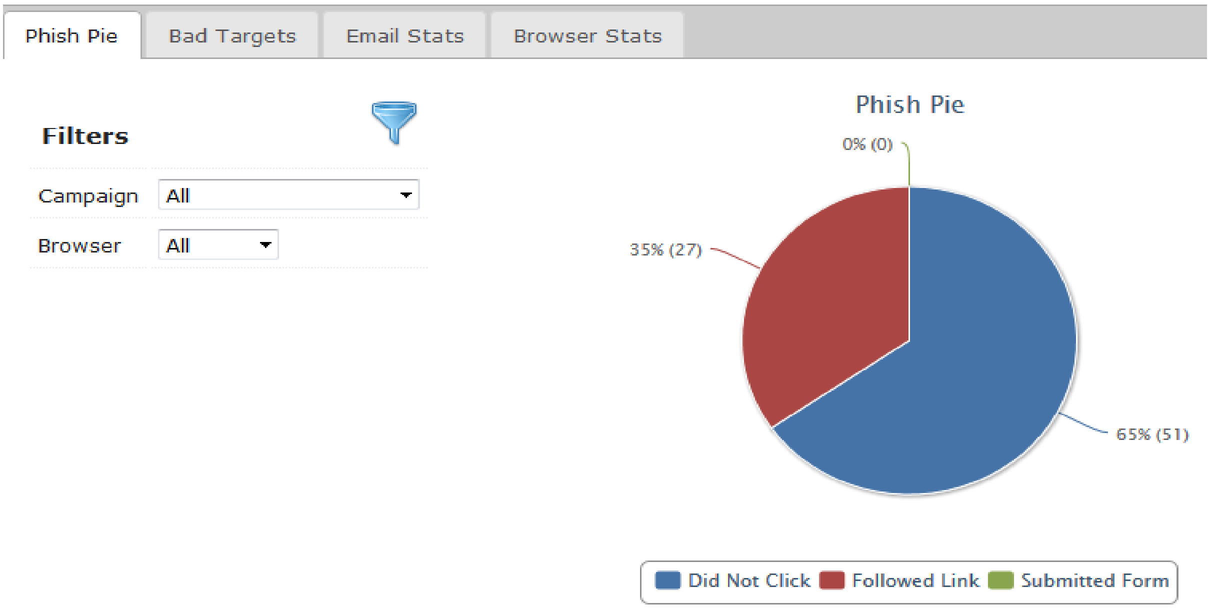
Upon login in, the admin can perform various tasks as described in the use. As a key function, the system has been coded to include a mailing functionality which is a key process of this solution in simulating attacks. This uses the PHP mailer() function and is configured to the IP of the local SMTP Server for mail forwarding.



```
    }
    if($ra['shorten'] == "TinyURL"){
        $shorten = "tinyurl";
    }
}
//get the next specified number of email addresses
$r = mysql_query ( "SELECT targets.fname AS fname, targets.lname AS lname, targets.email as email,
//send the emails
while ( $ra = mysql_fetch_assoc ( $r ) ) {
    //get this messages smtp host
    $host = $ra['relay_host'];
    $current_host = mysql_query("SELECT host, port, ssl_enc, username, aes_decrypt(password, '$sp
    while($ra_current_host = mysql_fetch_assoc($current_host)){
        $relay_host = $ra_current_host['host'];
        $relay_port = $ra_current_host['port'];
        $ssl_enc = $ra_current_host['ssl_enc'];
        if($ssl_enc == 1){
            $ssl = "yes";
        }else{
            $ssl = "no";
        }
        $relay_username = $ra_current_host['username'];
        $relay_password = $ra_current_host['password'];
    }
    //set the current email address
    $current_target_email_address = html_entity_decode($ra['email']);
    $current_target_email_address = preg_replace('/&#39;/', '\'',$current_target_email_address);
    $current_response_id = $ra['response_id'];
    $fname = $ra['fname'];
```

*Figure 20: Send email php file*

Figure below shows statistics captured from a simulated email attack.



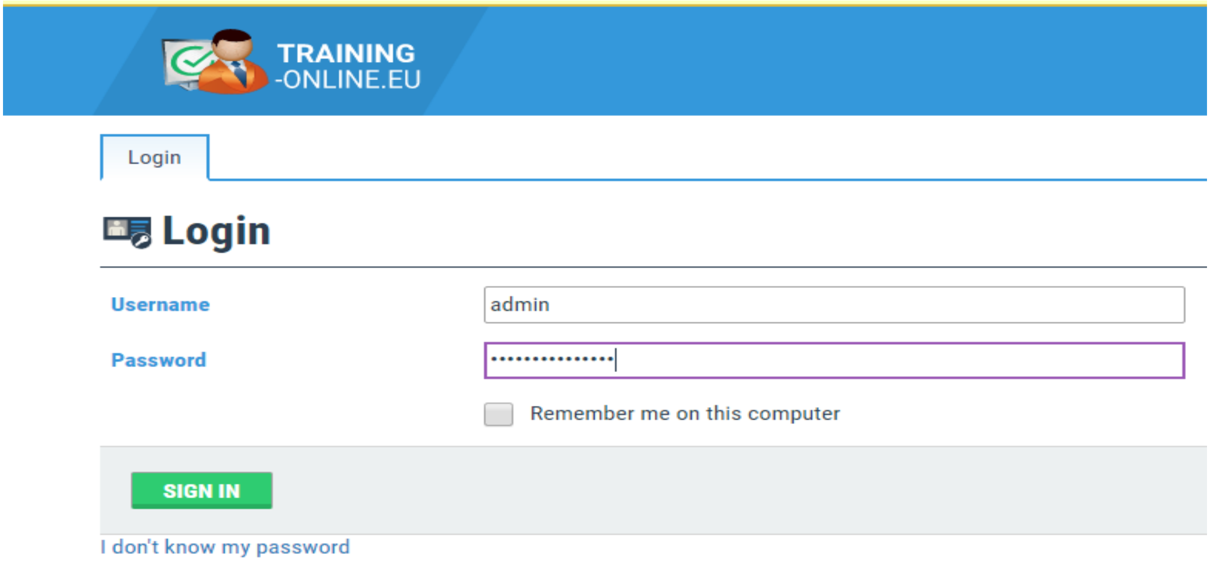
Filters

Campaign: All

Browser: All

*Figure 21: Simulated email statistics*

The Learning Management system that supported the above functionality to provide additional training where users can enrol themselves was outsourced due to resource and time constraints. The solution was developed using Moodle, an advanced Learning Management System Authoring Tool and was hosted on: **awareness.training-online.eu**



Login

Username: admin

Password: •••••••••••••••

□ Remember me on this computer

*Figure 22: Log in screen*

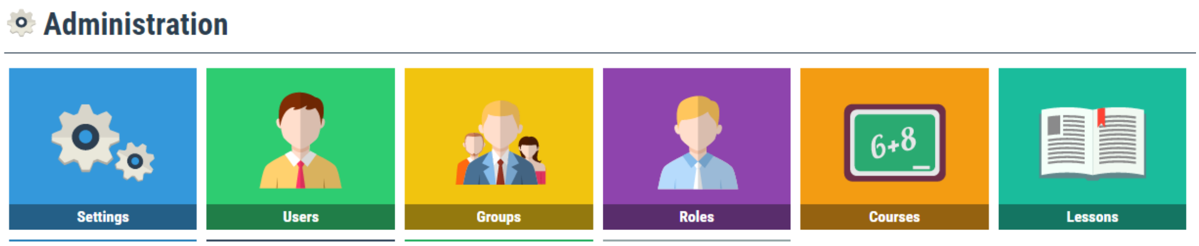
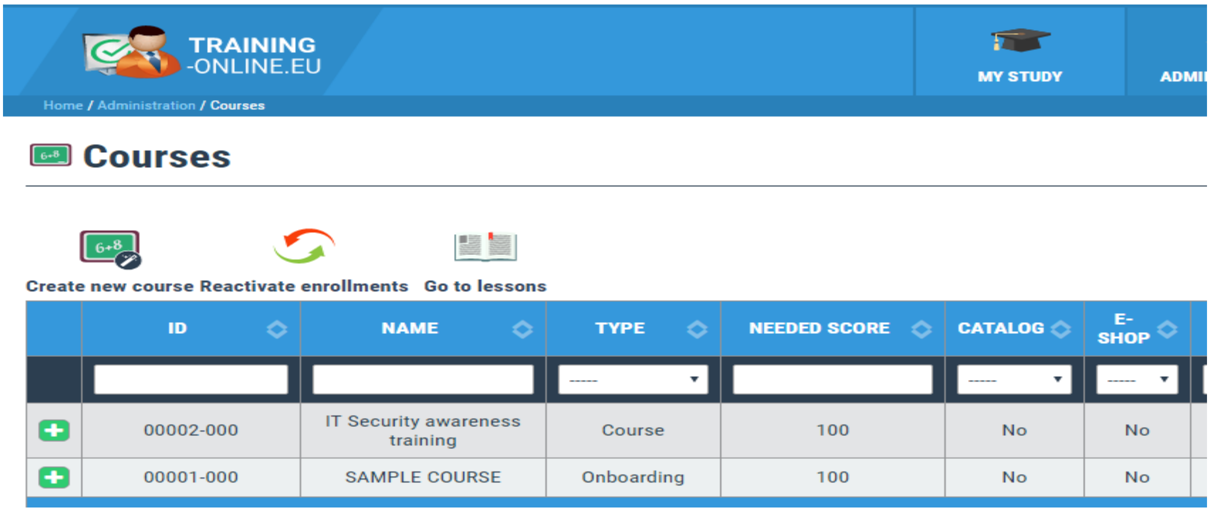


*Figure 23: Admin Panel*



| | ID | NAME | TYPE | NEEDED SCORE | CATALOG | E-SHOP |
|---|---|---|---|---|---|---|
| | | | ------ | | ------ | ------ |
| + | 00002-000 | IT Security awareness training | Course | 100 | No | No |
| + | 00001-000 | SAMPLE COURSE | Onboarding | 100 | No | No |

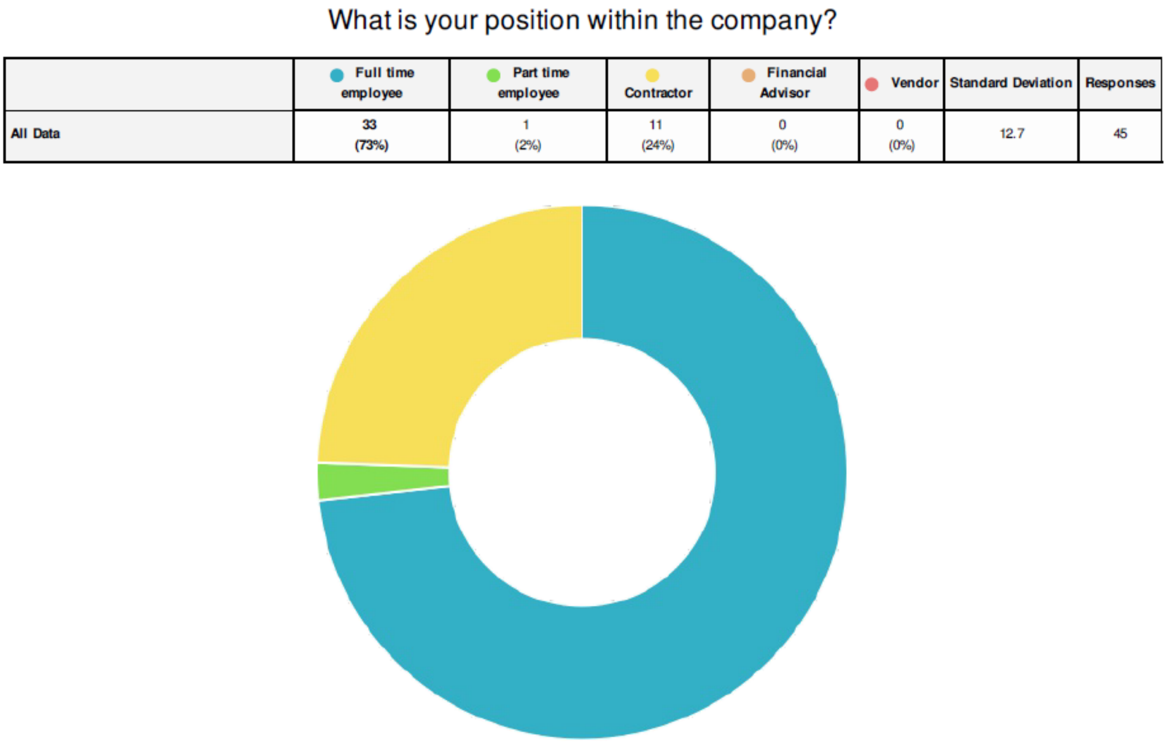
*Figure 24: Courses Screen*

# CHAPTER IV: RESULTS AND DISCUSSION

## 4.1 Survey Population and responses

The study used Britam Holdings Limited as the primary organization in research and study. The organization contains around 1000 employees either on permanent, contractual or part-time employees; and salesforce of over 3000 financial advisors (sales agents) who were not included in the study due to their limited interaction with the organizations Information Systems.

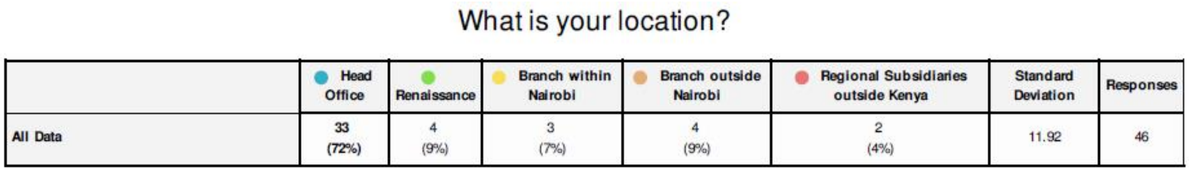
The 100 participants were selected using random sampling. The selection of 100 participants was a good representative of the entire population size of 1000. From the 100 sampled, questionnaires were sent through an online tool, 45 employees responded as shown below. The population was discerned using two categories location and role/position in the company. The head office had the highest number of respondents as was expected since majority of staff reside in the head office, a majority of the respondents were also fulltime employees, with contractors also significantly represented. We managed to get two responses from the regional subsidiaries.



What is your position within the company?

| | ● Full time employee | ● Part time employee | ● Contractor | ● Financial Advisor | ● Vendor | Standard Deviation | Responses |
|---|---|---|---|---|---|---|---|
| All Data | 33<br>(73%) | 1<br>(2%) | 11<br>(24%) | 0<br>(0%) | 0<br>(0%) | 12.7 | 45 |

*Figure 25: Role/Employment Type*



What is your location?

| | ● Head Office | ● Renaissance | ● Branch within Nairobi | ● Branch outside Nairobi | ● Regional Subsidiaries outside Kenya | Standard Deviation | Responses |
|---|---|---|---|---|---|---|---|
| All Data | 33<br>(72%) | 4<br>(9%) | 3<br>(7%) | 4<br>(9%) | 2<br>(4%) | 11.92 | 46 |

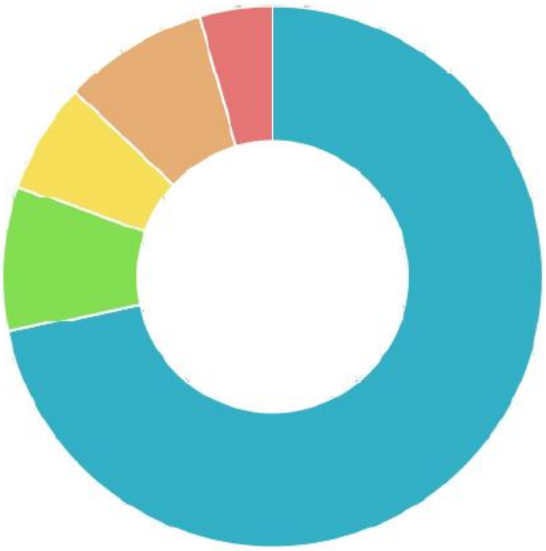
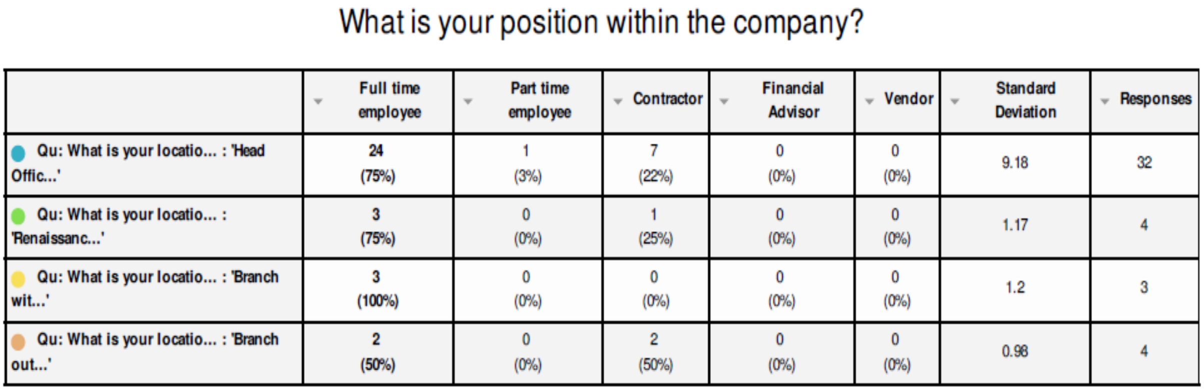


*Figure 26: Locations*

### *4.1.1 Comparisons of employee positions in the different locations*

In the different locations, we managed to collect responses from employees in different positions/employee types across the various locations; full time, part-time, contractors were all represented across the locations. However, we did not use the role/employee type comparison in analysing the awareness levels/risk scores since all positions/employee types should be equally Security aware. See the comparison of responses from different employee types in the different locations.



What is your position within the company?

| | Full time employee | Part time employee | Contractor | Financial Advisor | Vendor | Standard Deviation | Responses |
|---|---|---|---|---|---|---|---|
| ● Qu: What is your locatio... : 'Head Offic...' | 24<br>(75%) | 1<br>(3%) | 7<br>(22%) | 0<br>(0%) | 0<br>(0%) | 9.18 | 32 |
| ● Qu: What is your locatio... : 'Renaissanc...' | 3<br>(75%) | 0<br>(0%) | 1<br>(25%) | 0<br>(0%) | 0<br>(0%) | 1.17 | 4 |
| ● Qu: What is your locatio... : 'Branch wit...' | 3<br>(100%) | 0<br>(0%) | 0<br>(0%) | 0<br>(0%) | 0<br>(0%) | 1.2 | 3 |
| ● Qu: What is your locatio... : 'Branch out...' | 2<br>(50%) | 0<br>(0%) | 2<br>(50%) | 0<br>(0%) | 0<br>(0%) | 0.98 | 4 |

## 4.2 Processing and analysis of Results

This review comprised of 26 questions. A portion of the responses in this study showed solid awareness and great security rehearses while others demonstrated weak awareness, careless conduct, or high-hazard exercises. In light of these distinctions, each response in this overview (aside from the initial three inquiries) had been allotted a hazard score (1-5). "One" was the least hazard score and "five" was the most noteworthy hazard score. At the point when the after effects of the overview had been gathered, they were utilized to decide the general hazard score or hazard level of the organization as is indicated below.

- *For each of the 26 questions, increase each response hazard score (1-5) by the quantity of times it was picked by the review takers.*

  ***<response chance value> X <the number of times chosen> = <response total>***
- *Include the greater part of the response aggregates for a review total reaction summation.*
- *Divide the overall total response summation by the quantity of review takers to compute the study (or organization's) hazard score.*

  ***<cumulative reaction total>/<number of overview takers> = Organization's Hazard Score***
- *Utilizing the hazard score, check the "Hazard Levels" table underneath for the association's general hazard rating.*

***Table 2: Classification of Risk Levels***

| Risk Levels | Description |
|---|---|
| Low (25 – 39) | Employees know about great security standards and dangers, have been appropriately prepared, and conform to all authoritative |
| Elevated (40 – 60) | Employees have just been prepared on authoritative security guidelines and approaches, they know about dangers, yet may not take after great security standards and controls. |

| | |
|---|---|
| Moderate (61 – 81) | Employees know about dangers and know they ought to take after great security standards and controls, however require preparing on hierarchical security norms and arrangements. They additionally may not know how to recognize or report a security occasion. |
| Significant (82 – 96) | Employees don't know about great security standards or dangers nor are they mindful of or agreeable with authoritative security guidelines and arrangements. |
| High (97 – 110) | Employees don't know about dangers and nonchalance known security gauges and approaches or don't consent. They take part in exercises or practices that are effectively assaulted and misused. |

Using the above statistical formula, the organizational risk score was calculated as below.

***Table 3: Organizational Risk Level/Awareness Levels***

| | | |
|---|---|---|
| | **Cumulative Response Total** | 1731 |
| | **Number of survey takers** | 44 |
| **<cumulative response total> / <number of survey takers> = Organization's Risk Score** | | 39.34090909 |

The above organizational risk score represents responses from all survey takers across the organization; it shows the average risk level across the entire group. The result showed that the organizational risk score was 39.34; this was at the borderline of low and elevated risk level based on the risk levels table above.

For further analysis and dissertation, we proceeded to compute and compare the risk scores for the different locations to be able to get some business insight on the locations which have the highest risk score and potential to cause harm to the organization.

***Table 4: Risk Scores across the different locations***

| **Location** | **Risk Score** |
|---|---|
| All Locations | 39.34 |
| Head Office | 40 |

| | |
|---|---|
| Renaissance | 43.5 |
| Nairobi Branches | 38.67 |
| Branches outside Nairobi | 44.75 |
| Regional subsidiaries | 42 |

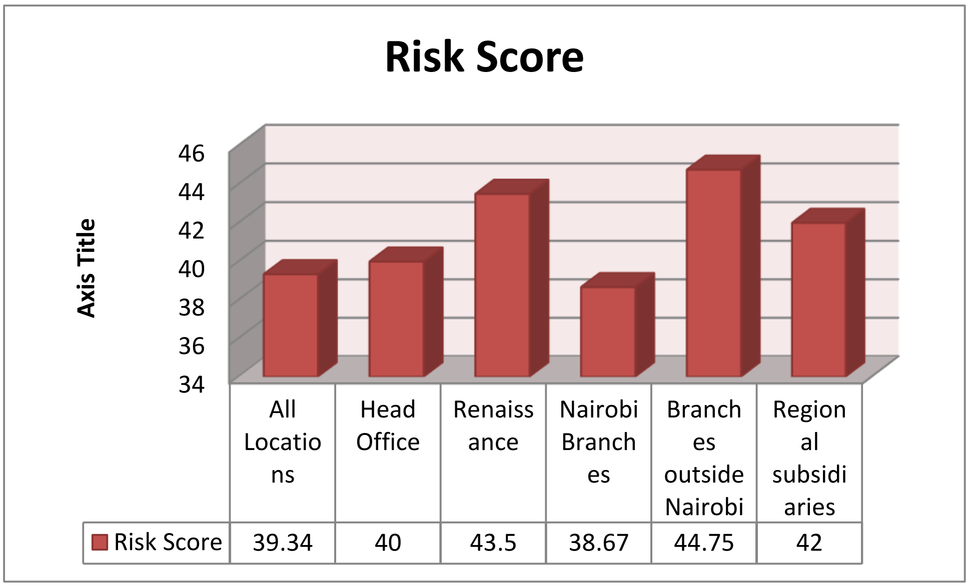
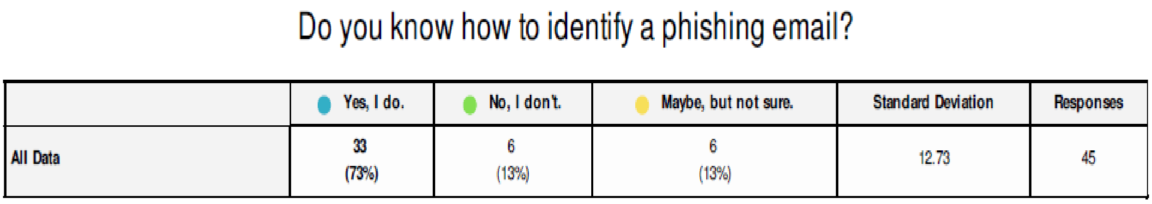


*Figure 27: Comparisons of Risk scores across the different locations*

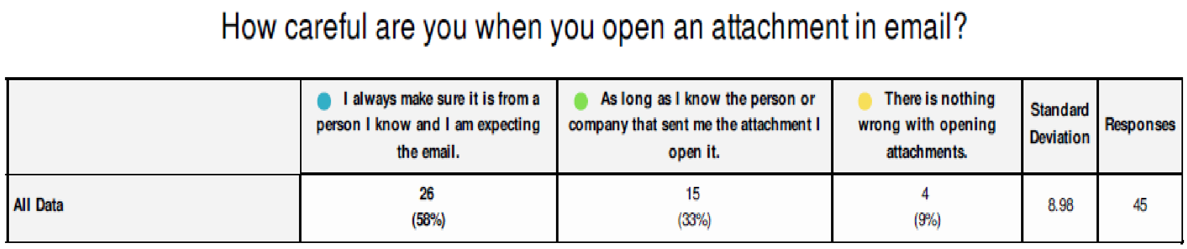
The average organizational risk score was 39.34, the head office which had the highest number of respondents had a risk score of 40. The head office risk score was almost marginally equal to the overall organizational risk score due to the fact that most respondents and most employees were from head office hence influencing the overall organizational risk score. The risk score of head office gave a risk level of elevated based on our classification table. From the responses collected, branches in Nairobi had the lowest risk score of 38 which is a low risk level, branches outside Nairobi and in the regions had risk scores of 44 and 42 respectively showing that current awareness training is not effectively addressing those locations hence the elevated risk level. Those locations posed the greatest risk to the company's information assets.

### *4.2.1 Comparison of responses for highlighted Security threat areas*



Do you know how to identify a phishing email?

| | ● Yes, I do. | ● No, I don't. | ● Maybe, but not sure. | Standard Deviation | Responses |
|---|---|---|---|---|---|
| All Data | 33<br>(73%) | 6<br>(13%) | 6<br>(13%) | 12.73 | 45 |



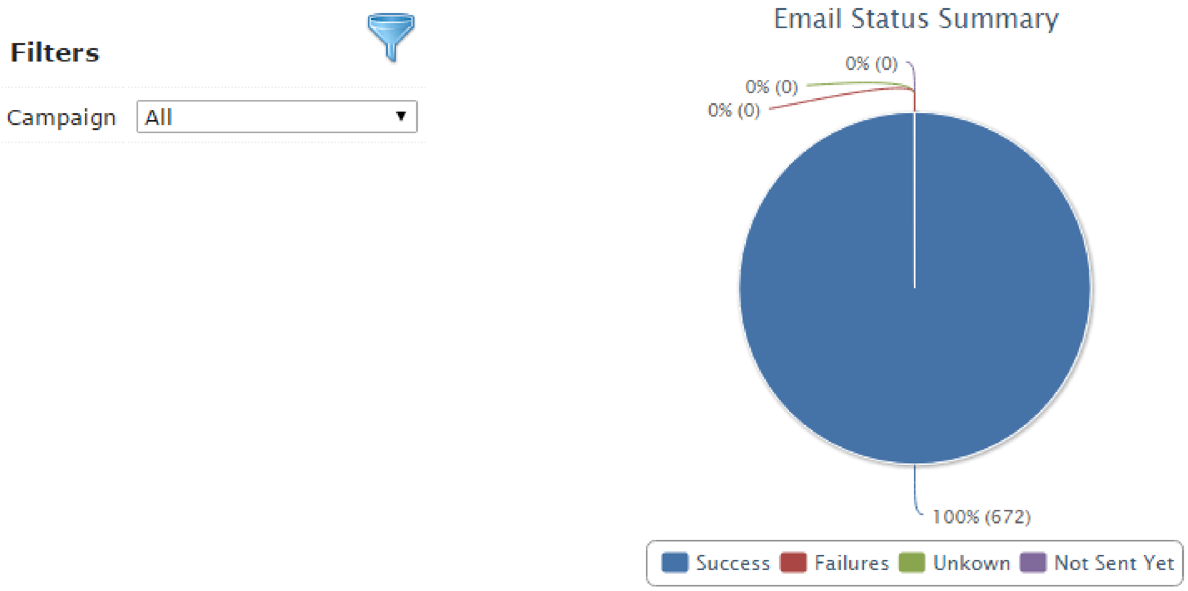
How careful are you when you open an attachment in email?

| | ● I always make sure it is from a person I know and I am expecting the email. | ● As long as I know the person or company that sent me the attachment I open it. | ● There is nothing wrong with opening attachments. | Standard Deviation | Responses |
|---|---|---|---|---|---|
| All Data | 26<br>(58%) | 15<br>(33%) | 4<br>(9%) | 8.98 | 45 |

The above results illustrated responses from employees on phishing and email scams. The first figure showed that majority of the respondents said they know how to identify a phishing email. The second figure however showed that quite a significant figure was not careful about how they responded to email attachments, and yet links and attachments are the main way that attackers use to deliver malicious packages and steal information.

### *4.2.2 Analysis and processing of system data*

The online phishing toolkit was used to simulate a phishing attack targeted at staff in the organization. A total of 672 emails were sent to staff in different Divisions of the organization. The phishing simulation was also able to identify the top riskiest targets.



Filters

Campaign: All

Email Status Summary

The diagram below shows the statistics of the simulation. The different departments and business units targeted showed different levels of ability to identify phishing emails and hence awareness levels with regards to email security.

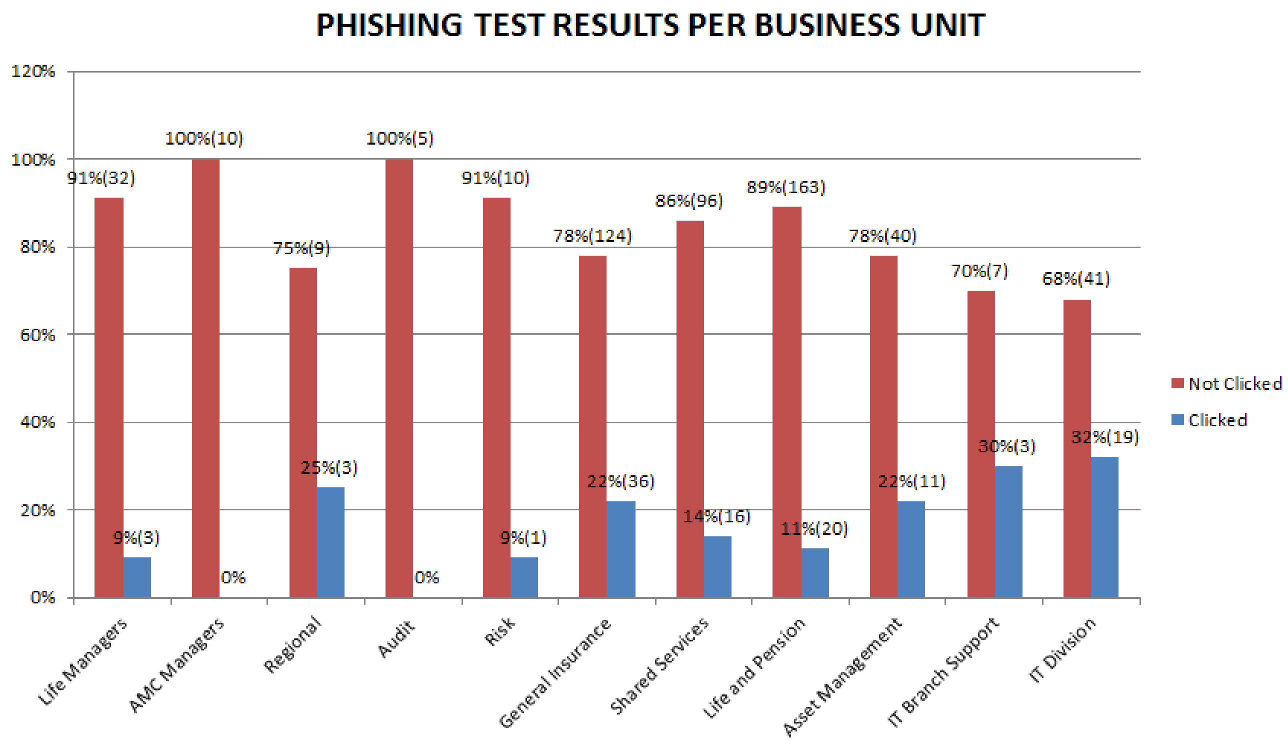
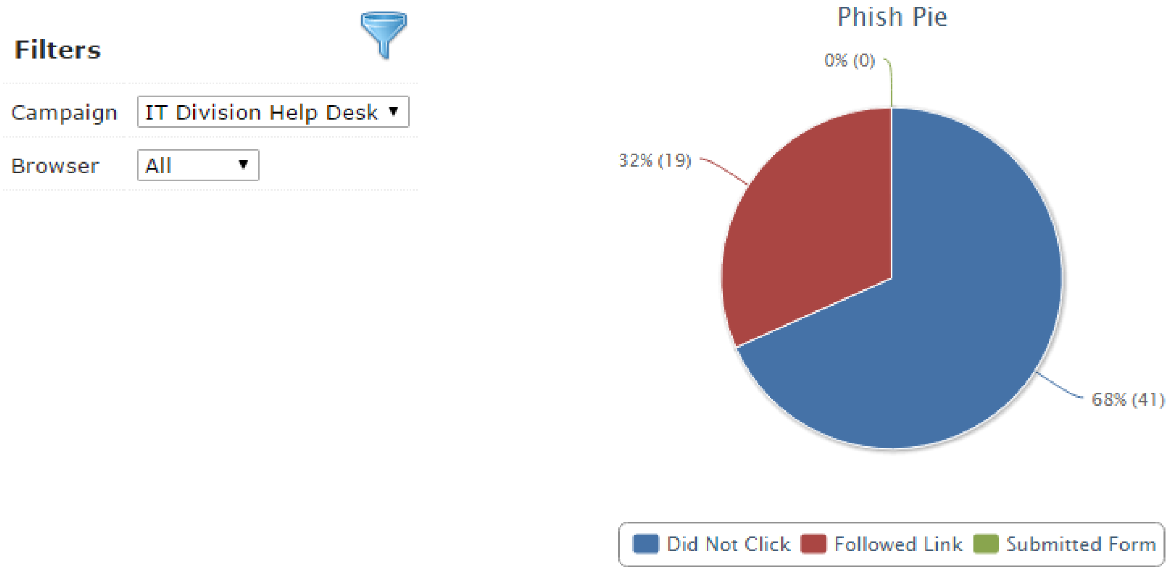


*Figure 28: Phishing Results/Business Unit*



Filters

Campaign: IT Division Help Desk ▼

Browser: All ▼

*Figure 29: IT Division Phishing Stats*

32% of IT recipients fell victim, these were IT staff who are trained and are expected to be aware and provide guidance for the normal non-technical users. If it was an actual attack, this means that 32% of Britam's IT team would be exposed. This can therefore be used as a reference point and metric on the awareness level of the targeted group. With time continuous tests can be used to show improvement on the awareness level and highlight individuals posing the highest threats to the organization. This corresponds to the results of the survey where 33% of those surveyed said that they would open/click an attachment as long as they knew the person or company that sent it. Attackers leverage such thinking and send emails that appear to come from people or organizations that you know.

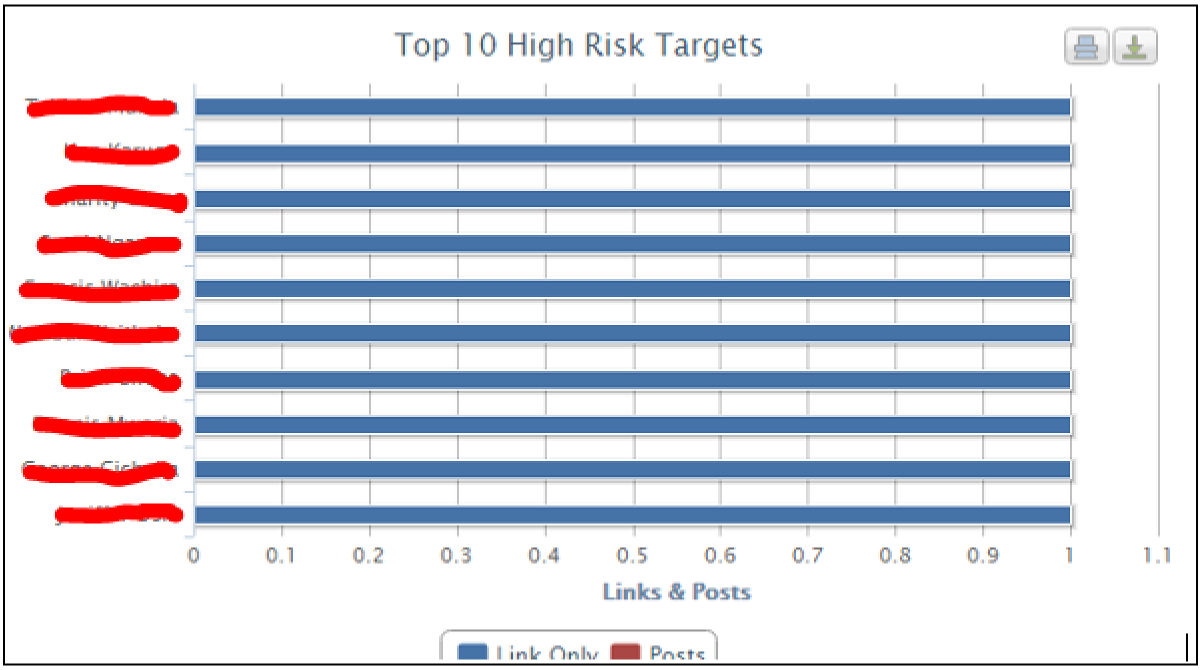


***Figure 30: Top 10 High Risk Targets***

# CHAPTER V: CONCLUSIONS AND RECOMMENDATIONS

## 5.1 Discussion

### *5.1.1 Purpose of Research*

At the beginning of the study, we set out to investigate the impact of technology, in the form of simulated phishing attacks, on the motivation of employees to undertake security awareness. The simulations were able to indicate the employees that fell victim to the simulated attacks and those that proceeded to undertake the awareness after a successful attack scenario. We also conducted a weighted survey with questions designed to measure a set of basic characteristics of the organization's security awareness posture and provide several metrics to measure the risk and awareness levels in the organization.

The detailed findings and results as per each objective are discussed in more detail below.

**Objective 1:** Investigate the impact of simulated phishing attacks on the motivation of employees to undertake an Information Security Awareness Program.

In our study, we sent out simulated phishing attacks targeted at employees of the organization. Upon delivery of the phishing email, there were three possible actions which the employees could take and which would be tracked by the system; first the employee could open the malicious email, second upon opening the email the employee could click on the phishing link or attachment which would indicate a successful attack, third after clicking the link, the employee would be redirected to a page informing them that the email was a simulated attack and they have fallen victim, they would then be prompted to enrol and take up an online IT Security Awareness Training.

The results as discussed in the results chapter indicated that most of the employees that fell victim enrolled for the Security awareness training. This indicated that as employees realized that they are quite vulnerable to such attacks, they were more motivated to take up the Security Awareness training that would help them comprehend such complex attacks, empower them with necessary skills and knowledge required to handle such attacks by identifying, preventing and reporting such attacks in the future.

To be able to achieve the above objective, we had to develop a phishing system. This was developed using PHP language for Scripting, HTML and CSS for markup and design, it was hosted on WAMP server and used MySQL Database managed through PhpMyAdmin, as has been discussed in more detail in the methodology chapter. The system provided the capability to design different phishing attack scenarios and send the phishing emails from different originating emails. It was able to track delivery of emails, which emails were successful and which ones bounced, it was able to capture who opened the phishing emails, who clicked on the phishing link and who proceeded to enrol and take up the online IT Security awareness training.

**Objective 2:** Conduct a weighted survey with questions designed to measure a set of basic characteristics of the organization's security awareness posture and provide several metrics to measure the risk and awareness levels in the organization.

The survey consisted of 26 questions designed to measure a set of basics characteristics of the organization's security awareness posture. Some questions collected factual data (role, location) while others collect data about the user's awareness, attitudes and behaviours. It gathered behavioural data on how users responded to threats, as well as data on attitudes and perceptions of organizational culture. We presented results on how this can help security training and awareness professionals gain a richer, more informed understanding of users' attitudes and habits within the context of their activities.

Using the metrics and statistical formulae discussed in the methodology and results chapters, the survey was able to provide metrics that can be used to calculate the risk levels/awareness levels in an organization. From the data collected, the organizational risk level was 39.34 which based on the classification levels, was at the borderline of low and elevated risk levels.

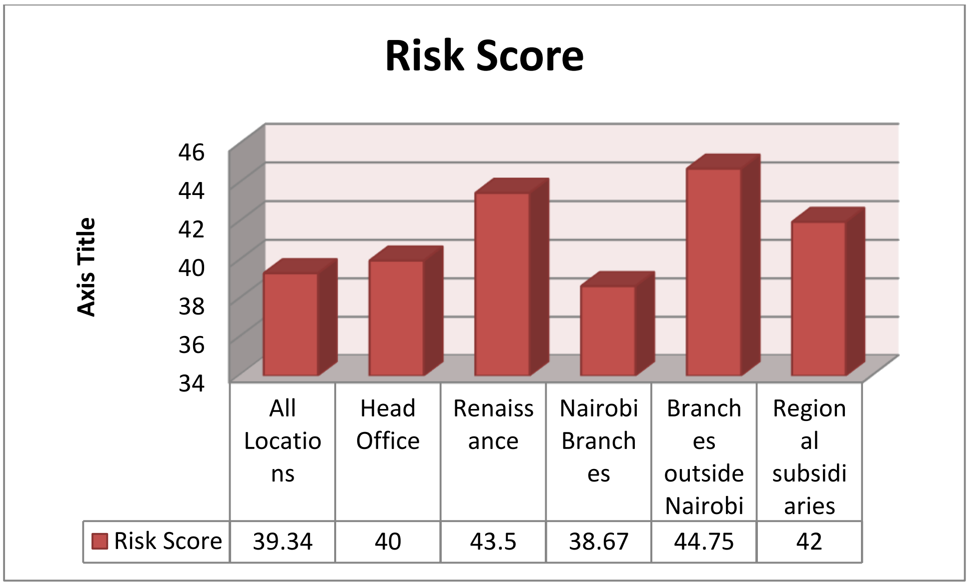


**Figure 31: Organizational Risk Scores**

**Objective 3:** Demonstrate how the results of the phishing attack simulations can provide metrics to measure awareness levels in an organization, impact, participation et al;

Upon completing the exercise, we gathered a lot of data from the system. This included the departments that were most prevalent in opening and clicking on phishing emails, the individuals who were most notorious for clicking on malicious emails; this could be used as a metric to identify which departments were more prone to specific types of phishing emails, and which users/departments were posing the most risk to the organization by clicking frequently hence may require more focused or specialized trainings.

The percentage of people who clicked the phishing link in the email against those who received the email and did not click may be used to some extent measure the levels of awareness in an organization. The number of users who participated in the awareness training after clicking the link could also be used as metric to track participation in security awareness initiatives. Also the numbers of those who clicked versus those proceeded to carry out the training could also be used to measure the impact of a phishing campaign towards motivating staff to carry out awareness training. The figures below show some of the statistics we received.

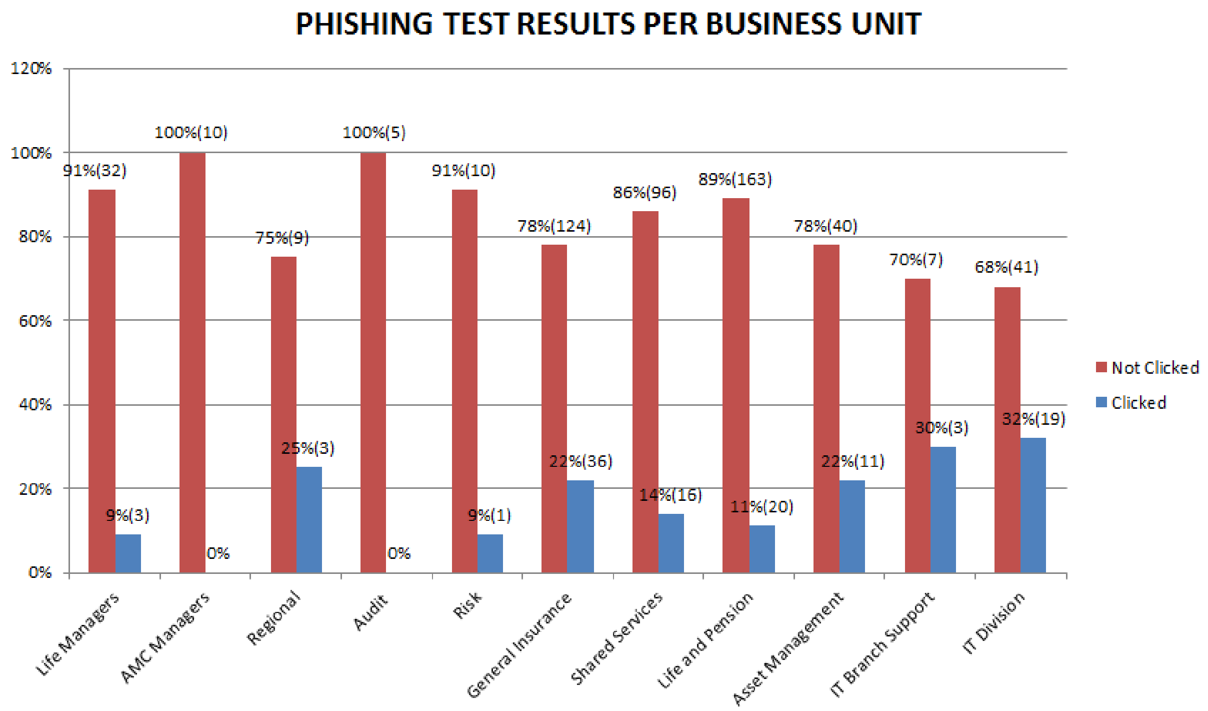
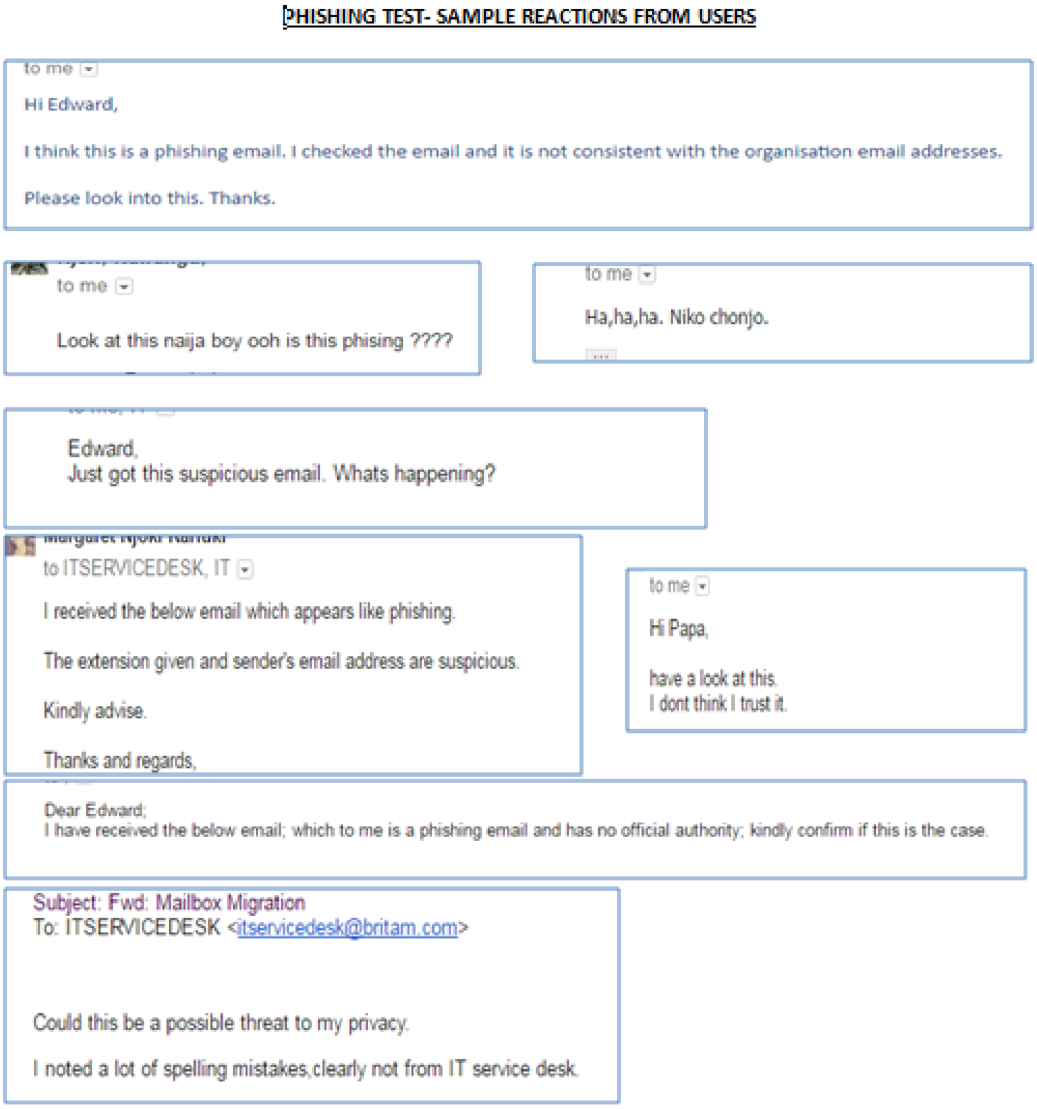


**Figure 32: Phishing Test results**



PHISHING TEST- SAMPLE REACTIONS FROM USERS

to me

Hi Edward,

I think this is a phishing email. I checked the email and it is not consistent with the organisation email addresses.

Please look into this. Thanks.

to me

Look at this naija boy ooh is this phising ????

to me

Ha,ha,ha. Niko chonjo.

Edward,
Just got this suspicious email. Whats happening?

Margaret Njoki Kariuki
to ITSERVICEDESK, IT

I received the below email which appears like phishing.

The extension given and sender's email address are suspicious.

Kindly advise.

Thanks and regards,

to me

Hi Papa,

have a look at this.
I dont think I trust it.

Dear Edward;
I have received the below email; which to me is a phishing email and has no official authority; kindly confirm if this is the case.

Subject: Fwd: Mailbox Migration
To: ITSERVICEDESK <itservicedesk@britam.com>

Could this be a possible threat to my privacy.

I noted a lot of spelling mistakes,clearly not from IT service desk.

**Figure 33: Sample Phishing Reactions**

## 5.2 Findings and Conclusions

The findings above showed that indeed technology did aid the IT security awareness program. The IT Security manager commended that the online simulation was an eye opener for him. He was able to identify the culprits who pose the greatest risks to information in the organization, he could tell which divisions in the organization posed the highest risk levels and could track who was taking part in the education.

Other findings in the research and development project showed that awareness levels vary across the different geographic locations of the organizations; the regions outside of Kenya had lower awareness levels hence posing risks to the organization. This is logical since the current IT Security team would be strapped in resources and finances to be able to train all the employees in the regions. This would be a good case for an automated security awareness program available online. The employees can then be able to take part by accessing it from their computers and they can be assessed together with other employees locally, giving them an opportunity to enrich themselves with Cyber Awareness skills.

### *5.2.1 Experience with Research Methodology*

The whole project experience was a challenging but interesting experience. It provided a chance to learn new principles, methodologies, concepts and ideas, and to apply the already acquired knowledge to solve real world problems. Time management was one of the best lessons learnt, we had to ensure that we are working within required prject timelines to avoid missing key deadlines for submissions and presentations. We had to align with our supervisors every so often and submit progress reports which ensured that we worked under a schedule. The project also promoted teamwork as we worked hand in hand with our fellow students to achieve the end goal and meet or exceed expectations.

The Research and development project provided an opportunity to get involved with research. This was a rather new field to some of us who have not experienced it before. It was quit liberating and enlightening but also came with its fair share of challenges.

Some of the benefits included:

1. Exposure to a wide array of information which was very eye opening providing information which I would not have easily come about.
2. Exposure to different types of literature from Scholarly articles to online journals to Institutional publications.
3. Getting versed with research techniques and methodologies.
4. Applying research design, data collection and data analysis principles.

However as mentioned, there were some challenges:

1. Too much information hence one is unable to filter out what is relevant.
2. Different schools of thought for the different literatures and hypothesis you come across, some will end up contradicting your own hypothesis.
3. Data collection; getting people to take their time to give your necessary data for your research.

4. Software development. Learning and implementing a programming language is quite a task and might be quite consuming.
5. It is very time-consuming to learn different tools and understand how to use tools with different application server and different configurations and deployments. Since the vendors' tools are inherently tied to their own application servers, and they don't work well with each other.

## 5.2 Recommendations

### *5.2.1 IT Security Awareness Material Should Be customized to fit different countries and Geographic Locations.*

It was noted that Security awareness levels varied across the entire group, the areas more remote from the Head office and in other regions/ countries of the organisations seemed to be fairing worse compared to staff in Nairobi and the Head Office. Material for training should therefore be organized such that it is customized to address the different locations and information security threats faced in those areas.

### *5.2.2 Metrics for Measuring IT security awareness levels need to be clearly defined*

If a phishing simulation attack is used to target employees, define some metrics to define the awareness levels, they may include:

1. How many people reported the attack?
2. What to report:
   - Report if you know you are being phished
   - Report if you don't know you are being phished
   - Report if you have fallen victim

### *5.2.3 Ensure there are at least two ways for users to identify the phish*

As you start your tests, you should ensure that the attack email has at least two or three ways for users to be able to identify that it is a phishing attack. Do not make the attack so complex that even aware users have a hard time identifying it. However, as you carry out more phishing tests in the future, increase the complexity to measure if users' behaviour and awareness levels are changing.

### *5.2.4 Click Results*

If a user falls victim to an email assessment, you have two main options:

- Give an error message which contains no feedback, this is especially good to give a baseline
- Give Immediate feedback which explains that it was a test, tells them what they did wrong and how they can protect themselves in the future. This is especially good for reinforcing key behaviours.

### *5.2.5 Violations*

When employees have violated policies by submitting company information to a simulated attack, the below actions can be taken.

- First violation: employee is notified and given additional or follow-up training
- Second violation: employee is notified and manager is copied
- Third violation: manager is required to have meeting with employee and report results to IT security
- Fourth violation: employee reported to HR for disciplinary action.

This are however guidelines and may vary depending on your organizations' IT security policies and procedures.

# REFERENCES

Burd, B. (2011). *Java For Dummies, 5th Edition.* Wiley.

Castro David Broshenka and Alfonso Peter. (2009). *Methods of Fact Finding.* Retrieved from FAO Coperate Document Repository: http://www.fao.org/docrep/Q1085E/q1085e07.htm

Cavanaugh, E. (2005). Web services: Benefits, challenges, and a unique visual development solution. Retrieved from www.altova.com.

Claburn, T. (2005). Machine wars: The battle between good and evil in cyberspace is increasingly fought with automated tools. *Information Week*, 54-63.

Daft, F. L., & Lengel, R. H. (1984). *Information richness: A new approach to manage information processing and organization design.* Greenwich, Connecticut: JAI Press.

Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *COMPUTERS & SECURITY*.

Dutton, J. (2017, September 26). *Three pillars of cyber security*. Retrieved from IT Governance UK: https://www.itgovernance.co.uk/blog/three-pillars-of-cyber-security/

E, S. (2001). Security training and awareness—fitting a square peg in a round whole. *Computers & Security, Vol. 23, Issue 1*, 1-2.

FAO. (2011). A guide for designing and developing e-learning courses. *E-learning Methodologies*.

Gartner Group. (2004). *Supply Chain Management: An International Journal.* Gartner Press.

Gartner, G. (2013). User Behavior Can Improve Security, but Only With Development and Practice. *Gartner Group*.

Harris, A., & Chen, C. C. (2009). The impact of information richness on Information Security Awareness Training. *Computers & Education*.

Javascripters. (2004). *Javascript: advantages and disadvantages*. Retrieved from JScripters.com: http://www.jscripters.com/javascript-advantages-and-disadvantages/

Johnston, J., Eloff, J. H., & Labuschagne, L. (2003). Security and human computer interfaces. *Computers & Security*, 675–684.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, 289–296.

Kruger, H., Drevin, L., & Steyn, T. (2009). A FRAMEWORK FOR EVALUATING ICT SECURITY AWARENESS.

Kruger, H., Drevin, L., & Steyn, T. (2009). A FRAMEWORK FOR EVALUATING ICT SECURITY AWARENESS.

Kruger, H., Drevin, L., & Steyn, T. (2009). A FRAMEWORK FOR EVALUATING ICT SECURITY AWARENESS. *North-West University-Potchefstroom Campus*.

Lappin, C. (2017, December 1). *Security Research and Strategy*. Retrieved from Threat Stack: https://www.threatstack.com

LaSalle, J. L. (2008). *Supply Logistics.* Huffman Publishers .

Minchington, C. (2011). The e-professional:embracing learning technologies. *Accountants for Business*.

Nabil Mohammed Ali Munassarand A. Govardhan. (2010). *A Comparison Between Five Models Of Software Engineering.* Retrieved October Monday, 2012, from www.IJCSI.org: www.IJCSI.org

Nielsen, J. (2000). Hard-to-use sites will fail. *The Irish Times*.

Oracle Technologies. (2008). *Object-Oriented Programming Concepts*. Retrieved September Monday, 2012, from oracle.com: http://docs.oracle.com/javase/tutorial/java/concepts/object.html

Php Basics Mysql. (2003). *phpbasics*. Retrieved from php.com: http://php.about.com/od/phpbasics/

Ponemon, I. (2012). *The Human Factor in Data Protection.* Ponemon Institute.

Rumbaugh, J. (1991). *Object Oriented Modeling and Design.* Prentice Hall,.

SANS. (2015, November). *securingthehuman*. Retrieved from SANS.org: https://securingthehuman.sans.org/blog/2015/04/07/cant-patch-stupidity-look-in-the-mirror

Schlienger, T., & Teufel, S. (2005). Tool supported management of information security culture.

Schlienger, T., & Teufel, S. (2005). Tool supported management of information security culture: An application to a private bank. *The 20th IFIP International Information Security Conference (SEC 2005) – Security and Privacy in the age of ubiquitous Computing*.

Schneider, E. C., & Therkalsen, G. W. (1990). How secure are your system? *Avenues to Automation*, 68-72.

Siponen, E. (2001). Five dimensions of Information Security Awareness. *Computers and Society*, 24-29.

Smirnova, S. (2012). *MySQL Querybook.* O'Reilly Media.

Sommers, K. Robinson, B. (2004). Security awareness training for students at Virginia Commonwealth University. *In the proceedings of the SIGUCCS'04, Baltimore, Maryland*, 379-380.

Sotiris Zigiaris-MSc BPR engineer. (2000). *Supply chain Management.* BPR HELLASSA.

Spearman, H. (2007). *Supply Chain Management.* NC & SA.

Stephanou, A., & Dagada, R. (2013). THE IMPACT OF INFORMATION SECURITY AWARENESS TRAINING ON INFORMATION SECURITY BEHAVIOUR: THE CASE FOR FURTHER RESEARCH. *University of the Witwatersrand*.

team, p. D. (2008). *Features*. Retrieved September Tuesday, 2012, from www.phpmyadmin.net: http://www.phpmyadmin.net/home_page/index.php

Valentine, J. A. (2006). Enhancing the employee security awareness model. *Computer Fraud & Security(6)*, 17–19.

van Niekerk, J. (2005). *Establishing an information security culture in organizations:*. Port Elizabeth: Nelson Mandela Metropolitan University.

Vigna, G. (2003). Teaching hands-on network security: testbeds and live exercises. *Journal of Information Warfare*, 8-25.

Walls, A., & Gartner. (2013). Effective Security Awareness Starts With Defined Objectives. *Gartner Group*.

Weatherspoon, R. (2006). Expansion of informal markets in Sub-sahara.

Whitman, M., & Mattord, H. (2005). Principles of information security. *2*.

# APPENDICES

1. Sample questionnaire and response analysis guideline

**1. What is your position within the company?**
a. Full time employee
b. Part time employee
c. Contractor
d. Financial Advisor
e. Vendor
Logic Note: Did not apply risk values to positions because they should all be equally security aware.

**2. What is your location?**
a. Head Office
b. Renaissance
c. Branch within Nairobi
d. Branch outside Nairobi
e. Regional Subsidiaries outside kenya
Logic Note: Did not apply risk values to locations because they should all be equally security aware.

**3. If from regional subsidiary, what is your country?**
a. Uganda
b. Tanzania
c. South sudan
d. Rwanda
e. Malawi
Logic Note: Did not apply risk values to locations because they should all be equally security aware.

**4. Do we have a security team?**
a. Yes, we have a company security team. (1)
b. No, we do not have a company security team. (4)
c. I do not know. (3)
Logic Note: Users who chose "C" are not informed and pose a risk for obvious reasons. Users who choose "B" when there really is a security team could represent an even higher risk to the organization because they believe they are aware but are really misinformed.

**5. Do you know who to contact in case you are hacked or if your computer is infected?**
a. Yes, I know who to contact. (1)
b. No, I do not know who to contact. (5)
Logic Note: Users who do not know who to contact when their PC is compromised pose a significant risk because they are likely to continue to use the device, potentially exposing the organization to further compromise or breach.

**6. Have you ever found a virus or Trojan on your computer at work?**
a. Yes, my computer has been infected before. (4)
b. No, my computer has never been infected. (2)
c. I do not know what a virus or Trojan is. (4)
Logic Note: Users who are unaware of malware threat pose a significant risk to an organization and would likely not know how or when to report it. Users who indicate they are aware of malware threat

but still have had infected work computers also pose a significant risk. Their activities and/or behaviours, while at work, may have led to the infections (sites they visit, links they click, etc.). However, the risk is slightly lowered because users who have been infected in the past are usually more security aware.

**7. Do you know how to tell if your computer is hacked or infected?**

a. Yes, I know what to look for to see if my computer is hacked or infected. (1)
b. No, I do not know what to look for to see if my computer is hacked or infected. (4)
Logic Note: Users who do not know what potential symptoms to look for are more likely to continue to use a compromised device, potentially exposing the organization to further compromise or breach.

**8. Have you ever shared your password from work with someone else?**

a. Yes (5)
b. No (1)
Logic Note: Users who are willing to share their work password are highly susceptible to social engineering or internal threats. The easiest way to get a password is to ask.

**9. Is the firewall on your computer enabled?**

a. Yes, it is enabled. (1)
b. No, it is not enabled. (5)
c. I do not know what a firewall is. (4)
Logic Note: Users who chose "C" are not informed and pose a significant risk for obvious reasons. Users who choose "B" are even a higher risk as they know what a firewall is and the protection it would provide; yet do not have it enabled.

**10. Is your computer configured to automatically update your security software?**

a. Yes, it is. (1)
b. No, it is not. (5)
c. I do not know. (3)
Logic Note: Users who chose "C" are not informed and pose a risk for obvious reasons. Users who choose "B" are even a higher risk as they know what "automatic updates" means and the protection it would provide; yet do not have it configured.

**11. How secure do you feel your computer is?**

a. Very secure (3)
b. Secure (1)
c. Not secure (4)
Logic Note: Users who feel their computer is not very secure may be right and the issue should be escalated to the responsible party. However, the user may be less likely to handle sensitive data or conduct risky transactions with it, which would lower the impact of compromise slightly. Users who feel their computer is very secure may be right and so the device poses little vulnerability risk to the organizations. However, the user may be more likely to handle sensitive data or conduct risky transactions with it, which would increase the impact of compromise. Cautious but aware users who chose "Secure" seemed like a good middle ground to strive for.

**12. Do you know what a phishing attack is?**

a. Yes, I do. (1)
b. No, I do not. (5)

Logic Note: Users who are aware of what phishing is are less likely to fall victim lowering risk.

**13. Do you know what an email scam is and how to identify one?**

a. Yes I do. (1)

b. No, I do not. (5)

Logic Note: Users who are aware of how to identify an email scam are less likely to fall victim lowering risk.

**14. 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. (1)

b. As long as I know the person or company that sent me the attachment I open it. (3)

c. There is nothing wrong with opening attachments. (5)

Logic Note: Users who choose "B" could be tricked into opening malicious attachments from spoofed sources that look like they came from recognizable persons or companies.

Users who choose "C" pose a significant risk to the organization because they are unaware of the threat, vulnerability or impact if they open a malicious attachment.

Cautious and aware users will choose "a".

**15. Do you know how to identify a phishing email?**

a. Yes, I do. (1)

b. No, I do not. (5)

Logic Note: Users who know how to identify phishing email are less likely to fall victim lowering risk.

**16. Is anti-virus currently installed, updated and enabled on your computer?**

a. Yes it is. (1)

b. No it is not. (5)

c. I do not know how to tell. (4)

d. I do not know what anti-virus is. (5)

Logic Note: Users who choose "B" may be indicative of users who are aware of what "anti-virus" is and the protection it provides, yet do not run or update it. This behavior may also indicate the user is risk tolerant and is more likely to improperly handle sensitive data or conduct risk transactions.

Users who choose "C" pose a significant risk because they are aware of what "anti-virus" is, but unaware of how to tell whether or not it is running.

Users who choose "D" pose a high risk because they are unaware of what "anti-virus" is and unaware of how to tell whether or not it is running.

**17. My computer has no value to hackers, they do not target me.**

a. True (5)

b. False (1)

Logic Note: Users who choose "A" pose a significant risk to the organization because they are unaware of the threat and impact if their computer is compromised.

**18. Are you aware of the company's IT Security Policies?**

a. Yes I am (4)

b. No I am not (1)

Logic Note: Users who choose “B” pose a significant high risk to the organization because they are unaware of the company security policies.

**19. Do we have policies on which websites you can visit?**
a. No, there are no policies, I can visit whatever websites I want while at work. (4)
b. Yes, there are policies limiting what websites I can and cannot visit while at work, but I do not know the policies. (2)
c. Yes, there are policies and I know and understand them. (1)
Logic Note: Users who choose “B” are protected by corporate filtering solutions, but are an elevated risk because they are unaware of the policies.
Users who choose “A” pose a significant risk because they can visit whatever site they want including potentially malicious sites.

**20. Do we have policies on how what you can and cannot use company email for?**
a. No, there are no policies, I can send whatever emails I want to whomever I want while at work. (4)
b. Yes, there are policies limiting what emails I can and cannot send while at work, but I do not know the policies. (2)
c. Yes, there are policies and I know and understand them. (1)
Logic Note: Users who choose “B” are protected by corporate filtering solutions, but are an elevated risk because they are unaware of the policies.
Users who choose “A” pose a significant risk because they can visit whatever site they want including potentially malicious sites.

**21. Can you use your own personal devices, such as your mobile phone, to store or transfer confidential company information?**
a. Yes I can. (5)
b. No I cannot. (1)
c. I do not know. (4)
d. Yes I can, if using the company provided solution. (2)
Logic Note: Users who choose “A” represent a high risk to the organization because there is little if any control over the processing, transmitting, or storing of sensitive data on personal devices.
Users who choose “C” pose a significant risk because at minimum they are unaware of whether or not it is allowed, and they are more likely to handle confidential information on personal devices without knowing.

**22. Has your boss or anyone else you know at work asked you for your password?**
a. Yes, they have (4)
b. No, they have not. (1)
Logic Note: Organizations where it is common and accepted for others to ask users for their passwords is more likely to be successfully attacked with social engineering.

**23. Do you use the same passwords for your work accounts as you do for your personal accounts at home, such as Facebook, Twitter or your personal email accounts?**
a. Yes I do. (4)
b. No I do not. (1)
Logic Note: When third party accounts are compromised, users who use the same password on work as personal accounts are much more vulnerable to password attacks and guessing.

**24. How often do you take information from the office and use your computer at home to work on it?**

a. Almost every day. (5)
b. At least once a week. (4)
c. At least once a month. (2)
d. Never (1)

Logic Note: Users who answer “A”, B”, or “C” pose an increasing risk of data loss to organizations based on increasing frequency and the use of a home personal computer.

**25. Have you logged into work accounts using public computers, such as from a library, cyber café or hotel lobby?**

a. Yes, I have (4)
b. No, I have not (1)

Logic Note: Users who access work accounts from public computers are more likely to have their credentials or corporate data stolen if these devices are insecure or compromised. This would also indicate the user is not aware of the potential risks of doing so.

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

a. Yes I have. (2)
b. No I have not. (1)

Logic Note: Users who choose “A” pose a higher risk to the organization than those who choose “B” because they are more likely to download malicious software and infect a work computer.