2019

# Employee awareness on social engineering threats in the financial sector

Francis Mwangi Wokabi
*Faculty of Information Technology (FIT)*
*Strathmore University*

# Employee Awareness on Social Engineering Threats in the Financial Sector

**Wokabi Francis Mwangi**

**Master of Science in Information System Security**

**2019**

# Employee Awareness on Social Engineering Threats in the Financial Sector

**Wokabi Mwangi Wokabi**

**Submitted in Total Fulfilment of the Requirements for Award of the Degree of Master of Science Information Systems Security at Strathmore University**

**Faculty of Information Technology**

**Strathmore University**

**Nairobi, Kenya**

**June, 2019**

## Declaration

I declare that this work has never been previously submitted and approved for the award of a degree by this or any other university. To the best of my knowledge and belief, this dissertation contains no material previously published or written by another person except where due reference is made in the proposal itself.



Wokabi, Francis Mwangi

18th June 2019

**Approval**

This dissertation of Wokabi, Francis Mwangi was reviewed and approved by the following:

Dr, Humphrey Njogu,
Senior Lecturer, Faculty of Information Technology,
Strathmore University.

Dr, Joseph Orero,
Dean, Faculty of Information Technology,
Strathmore University.

Professor Ruth Kiraka,
Dean, School of Graduate Studies,
Strathmore University.

## Abstract

Despite the great gains that have been achieved through use of the Internet, a lot of threats have also emanated in equal measure from its increased usage. Some of the threats are largely associated with cyber-attacks. From identity theft, phishing, tailgating, shoulder surfing and google hacking among others. Generally, most of these attacks would typically begin with the very basic stage or phase known as social engineering. Financial institutions are at high risk today as attackers use various forms of attacks to social engineer the employees that work in the financial sector. The use of trickery and deception by cyber criminals to gain the trust of employees has made them the most vulnerable element of a computer system.

The aim of this study was to identify the various forms of social engineering attacks in the financial sector and to develop a web-based assessment tool that will enable financial institutions to enhance the preparedness of their employees by assessing their awareness levels with respect to social engineering threats. The tool was used to achieve this by administering assessment tests to employees and the results from the assessment tests were used to determine training requirements for the employees. The proposed tool was developed using the Rapid Application Development (RAD) approach or methodology through a series of continuous testing and integration phases to ensure that the final product met the specified requirements. The results from the testing phases of the development revealed that the system is robust enough to handle requests from more than 80 users and it's performance is not degraded even as the number of users increase. The system has an accuracy rate of 100% when it comes to scoring questions. In addition to this, the tests showed that the system has an overall average response time of between one to five minutes when responding to user requests.



**Key Words:** Assessment, Cybersecurity, Phishing, Rapid application development, Threats.

# Table of Contents

# Table of Figures

## Acknowledgements

I would like to acknowledge my supervisor Dr Humphrey Njogu for his supervision and dedication towards helping prepare this study. I would also want to acknowledge my wife, Linet Wawira Mwangi for the support she has given as I spent sleepless nights working hard to come up with this dissertation document. Finally, I want to thank the almighty God for giving me the grace, courage and strength to finish the race.

## List of Abbreviations

| | | |
|---|---|---|
| **ATM** | - | Automated Teller Machine |
| **ATP** | - | Advanced Persistent Threat |
| **CD** | - | Compact Disc |
| **DFD** | - | Data Flow Diagram |
| **DoS** | - | Denial of Service |
| **ERD** | - | Entity Relationship Diagram |
| **GB** | - | Gigabyte |
| **GHZ** | - | Gigahertz |
| **HTTP** | - | Hyper Text Transfer Protocol |
| **IPS** | - | Intrusion Prevention System |
| **IT** | - | Information Technology |
| **LAN** | - | Local Area Network |
| MBPS | - | Megabytes Per Second |
| **MITM** | - | Man-In-The-Middle-Attack |
| **NIA** | - | National Intelligence Agency |
| **OAIC** | - | Office of the Australian Information Commissioner |
| **OS** | - | Operating System |
| **PKI** | - | Public Key Infrastructure |
| **RAD** | - | Rapid Application Development |
| **SEDF** | - | Social Engineering Defence Framework |
| **SQL** | - | Structured Query Language |
| **SSL** | - | Secure Socket Layer |
| **TB** | - | Terabyte |
| **URL** | - | Uniform Resource Locator |
| **VPN** | - | Virtual Private Network |

# Chapter 1: Introduction

## 1.1 Background of the study

According to Morgan (2017), cybercrime will cost the world in excess of $6 trillion annually by 2021 and will continue to be one of the greatest challenges that humanity will face for the next two decades. The effects of cybercrime such as loss of sensitive data, identity theft, disruption to normal business operations and embezzlement of funds are not only damaging but they result in loss of revenue for any organisation to very great proportions. Attacks such as Denial of Service (DoS), identity theft, password cracking, email phishing and man-in-the-middle (MITM) attacks are continually becoming a thorn in the flesh for most information technology (IT) security teams in most organisations. It does not help that the type and nature of these attacks continue to grow in cost, size and sophistication (Morgan, 2017). Increased cyberattacks have seen successful breaches per company rise to more than 27% annually with incidents like Petya and WannaCry causing heavy disruption of services and affecting very large corporations globally in 2017 (The Ponemon Institute, 2017). Some of these attacks can be aided heavily by the attacker's ability to persuade or trick employees to give out or reveal information about the organisation that could lead to a compromise. The attackers are largely able to achieve this through social engineering attacks (The Ponemon Institute, 2017).

Social engineering refers to the manipulation of individuals by preying on their psychological and emotional aspects to gain access to restricted areas or obtain sensitive information for malicious purposes. Because humans are the weakest link in the security chain, cyber criminals can prey on common aspects of human psychology such as curiosity, courtesy, gullibility, greed, thoughtlessness, shyness and apathy (Chizari, 2015). According to Airehrour (2018), there are several causative factors for social engineering attacks, and these are classified as demographic, organisational and human factors. The demographic factors cover issues such as a person's gender, age, personality and culture. For instance, due to their love for shopping, women may be more susceptible to respond to junk emails or digital media that contain advertisements from commercial websites offering various products at discounted rates. It has become increasingly important today for organisations globally to train their staff on cyber security awareness as way of mitigation for social engineering attacks (Airehrour, 2018)

Organisational factors such as poor or insufficient security policies can make an organisation vulnerable to various attacks. In addition to this, lack of proper and effective training for employees on information security awareness enables attackers to prey on ignorant unsuspecting employees in their bid to gather sensitive information about the organisation. Employees must be therefore be thoroughly and continuously trained on how to identify various social engineering attacks and how to avoid them. They also need to be trained about being careful who they share their personal data with as well as any sensitive information related to the company. If this kind of training is not given to them then it becomes very easy for an attacker to socially engineer an unsuspecting victim by tricking them into giving out sensitive data or information that may enable the attacker to compromise an organisations system and eventually get hold of their data (Airehrour, 2018).

According to Avenassian(2017), one of the most sophisticated threats that continue to face the financial sector today is social engineering. The sector has become a high value target for attackers due to the highly sensitive nature of financial data. Cyber criminals are now using emails, social media, attachments, phone calls and various mediums of communication to deceive employees within organisations into giving out their confidential details such as their account details, usernames and passwords. To make matters worse, financial institutions believe that they are much more secure than the average company because they comply to the stringent regulations that have been put in place by governments especially within the banking industry (Avanessian, 2017)

The goal for pursuing this study was to demonstrate the need for organisations in the financial sector to invest heavily in information security awareness training for staff and to create a case for the development of a web-based cybersecurity assessment tool that can help organisations mitigate against the threat of social engineering attacks by testing or analysing the knowledge.

### 1.2 Problem Statement

Most social engineering attacks do not require any form of technical experience to execute. As a result, organisations within the financial sector remain vulnerable as their employees are oblivious to the cyber threats that exist out there. Cyber criminals take advantage of the fact that financial institutions rarely invest in some form of cyber awareness training for their people. Due to this flaw, the human factor in the security chain becomes the most exploited weakness. Irrespective of how much investment is made in Information Technology (IT)

security solutions, if employees within the financial sector are not empowered through regular training and awareness campaigns, then the attacker will always have the upper hand (Serianu, 2017). Social engineering attacks form the basis or root of most attacks since the success of such attacks is largely dependent on human or employee factors like ignorance, mood, perception among others. The volume and value of transactions within the financial sector have increased tremendously due to advancements in technology. As a result, security of these transactions has become a great concern. Cyber criminals have been known to make use of various social engineering techniques to convince bank employees and customers to give away their personal details as well as access to sensitive financial data. One of the most common attacks used by criminals is the spear phishing attack where a targeted email is sent to employees or a group of employees with high level access with the aim of deceiving them into clicking on a malware laced attachment thus granting the attacker access to their user accounts (Schaffer, 2018). As a way of mitigating such attacks, financial institutions need to adopt various approaches that can ensure a continuous internal assessment of their employees' level of preparedness with the goal or aim of identifying the training gaps that exist. Most of the current methods of mitigating against forms of social engineering attacks focus more on preventive controls as well as simulation of email phishing attacks and do not have the capability of carrying out a knowledge assessment exercise through a series of probing questions hence they lack the ability to identify training gaps among employees. In addition to this, the current mitigation techniques cannot effectively detect the employees who require further training (Airehrour, 2018). This study ensures that organisations in the financial sector place a lot of emphasis on the need to train their staff about forms of social engineering attacks and continually assess their resilience levels.

### 1.3 Research Objectives

The main purpose of this study was to design, develop and test a web-based automated assessment tool to create awareness on forms of social engineering attacks targeting employees in the financial sector.

The specific objectives of this study were to:

1. Determine common social engineering attacks that target employees in the financial sector.
2. Review the existing solutions for addressing forms of social engineering attacks.

3. Design, develop and test a web-based automated assessment tool to create awareness on forms of social engineering attacks targeting employees in the financial sector.
4. Validate the effectiveness of the proposed solution towards creating employee awareness on social engineering attacks in the financial sector.

### 1.4 Research Questions

1. What are the common forms of social engineering attacks that target employees in the financial sector?
2. What are the strengths and weaknesses of the existing tools for addressing forms of social engineering attacks against employees?
3. How will the proposed automated tool be designed, developed and tested?
4. How effective will the proposed solution be towards addressing social engineering attacks?

### 1.5 Significance of the study

This study was necessary because it will make organisations within the financial service industry aware about the serious threat of social engineering attacks and enable them to realise the importance of training their employees as one way of mitigation against these kinds of threats. The study also resulted in the development of a web-based employee assessment tool that can be used by financial institutions to evaluate the cyber strength and preparedness of their staff and identifying the training gaps that exist within the organisation regarding social engineering attacks.

### 1.6 Scope and Limitations

This study focused primarily on the forms of social engineering attacks against employees from organisations within the financial sector. Special focus was directed towards highlighting the threats that these organisation face by failing to properly and thoroughly train their staff about social engineering attacks. The proposed web-based tool was restricted towards identifying gaps through employee awareness assessments that would result in various training recommendations for different employees based on the outcome of the audit.

# Chapter 2: Literature Review

## 2.1 Introduction

This chapter explores in depth how social engineering attacks are on the rise especially within organisations in the financial service sector and how these attacks are targeted at employees. This section also explores the various types of social engineering threats as well as the pros and cons of existing automated solutions that are currently being used to mitigate against such attacks.

## 2.2 Cybersecurity

According to Babate (2014), cyber threats are growing at an alarming rate and at the same pace with the online use of personal computers and mobile devices. It is evident that cyber security is becoming a matter of priority for all organisations who intend to remain competitive and vibrant within the global market. This seems to have greatly watered down the perceived benefits of various forms of technology (Alhaji Idi Babate, 2014). This has been worsened by the fact that cyber criminals have come up with more sophisticated approaches of attacking an organisation's assets. One such approach is the social engineering attack which generally preys on the trust element of the human nature in order to persuade or trick employees into revealing sensitive information about the organisation with or without the use of technology (Chizari, 2015).

According to the IBM cost of data breach report of 2018, the average total cost of a breach in the United States of America was $7.91 million while in the Middle East it was $5.31 million. In addition to this, the average global cost per record of resolving an attack was $157 (IBM, 2018). Further to this, studies reveal that on average, cyber-crime is costing organisations globally about $11.7 million. Consequently, the number of successful breaches globally has gone up by more than 27% especially after WannaCry and Petya ransomware adversely affected large corporations across the globe. A recent breach involving Equifax, a consumer credit reporting agency resulted in the theft of 143 million records belonging to its customers (Accenture, 2017).

## 2.3 Information Security in the Financial Sector

In most organisations today, information is a very vital asset that contributes towards the overall success and competitiveness of a business. It is therefore very important for all

organisations to put more effort towards preserving the confidentiality, integrity and availability of their data. It is imperative for most companies to come up with or establish very robust information security strategies which need to be incorporated into the overall business strategy. Previously, security has mostly been geared towards blocking unauthorised or illegitimate access of data. However, due to the changing nature of cyber threats, it is not enough to use preventive measures in isolation, but organisations must now adopt ways of detecting as well as responding to security threats and breaches (Purdy, 2016).

According to Purdy (2016), organisations globally need to make strong commitments at all levels within their structure in their efforts to address cyber security risks. In addition to this, they must continuously find ways of incorporating the same in their risk management activities. The risk management process requires active involvement from the senior management level, all the way to the bottom of the food chain in order to guarantee a higher rate of success in the war against cyber threats. All the key departments and functional components need to have in place their specific security requirements that need to be strictly adhered to by staff. These requirements need to be integrated in to the overall day to day business operations of the organisation followed up by a rigorous annual review mechanism to determine their effectiveness or otherwise (Purdy, 2016).

The use of modern technology has greatly favoured a lot of organisations and more so those in the financial sector. A host of services such as digital cash, networking and information storage have greatly facilitated the expansion and exponential growth of financial institutions. However, it would be quite disastrous to be oblivious to the fact that financial institutions are under grievous threat from the rise of sophisticated cyber-attacks. According to Sachkov (2017), close to 99% of global cyber-attacks involve money theft through targeted attacks on banks. This is further validated by the fact that losses suffered through targeted attacks on financial institutions rose by almost 300% in 2016. These attacks are executed through use of regular ready-to-use tools purchased from underground hacking forums or readily available software on the web which is free and hence they do not require any special experience on the part of the attacker (Sachkov, 2017).

Most companies do not understand how these attacks are carried out and they are therefore unable to develop appropriate counter measures or mitigation approaches. In addition to this,

financial institutions rely too much on conventional security features like firewalls, intrusion detection/prevention solutions, updated operating systems (OS) and up to date antivirus programs to stop intruders from accessing their network and infrastructure. What they fail to understand is that all these measures in isolation are not enough to stop attackers and that what is required is an all-inclusive strategy that emanates all the way from the top management to the operational staff within the company. All employees must therefore be taken through a rigorous training and awareness program which include simulated phishing attacks as well as knowledge about social engineering attacks that can help them to know how to respond in various situations or in the eventuality of a real attack. The recruitment process within organisations in the financial sector must also be carried out very carefully to allow for proper vetting of the recruits and thorough background checks to ensure that rogue individuals are not absorbed into the workforce. This together with very strict policies and regulations that are embedded within the overall company policy would guarantee a higher rate of success against cyber threats. Although there is no way of guaranteeing 100% protection against attacks on financial institutions, the risks can be mitigated by improving the efficiency of the organisation's security strategy or approach (Sachkov, 2017).

On the global scene, financial institutions continue to face a major risk when it comes to cyber-crime. For instance, in 2016 alone, distributed denial of service attacks on financial institutions rose to 56%. In that same year, cyber criminals managed to steal about $1.3 billion from 100 banks in 30 countries over an eighteen-month period using spear phishing techniques targeted at high level employees via malware attacks. In some cases, automated teller machines (ATM's) were manipulated to dispense large amounts of cash. In such cases, it can cost a financial company about $1.8 million to recover from cyber-attacks which can bring critical business operations such as online banking to a halt (SentinelOne, 2016).

Locally, data from various studies indicate that financial institutions in Kenya lost KES 21 billion in to cyber-attacks in 2017 as banks and micro-finance institutions continue to adopt digital products as a way of staying competitive and enhancing customer experience (Wainainah, 2019). The Sacco Cyber Security Report (2018) reveals that 64% of saccos do not take their employees through any form of cybersecurity awareness training or in some cases the training would only be carried out when a breach or incident occurs. In addition to this, 97% of saccos spend less than US$ 10,000 on mitigation of cyber threats. This is further

compounded by the fact that 97% of them experience a massive shortage of IT staff with information security skills (Serianu Limited, 2018).

### 2.4 Common threats and vulnerabilities in the Financial sector

Regulators around the globe are now more awake to the fact that financial institutions are increasingly facing major threats from cyber criminals despite taking major steps towards strengthening their internal security mechanisms. Consequently, the speed at which technology keeps changing and the evolving nature of cyber threats continues to make things worse for such organizations. According to the Sacco cyber security report (2018), the most common attacks targeting institutions in the financial sector are data breaches, abuse of privileged access, critical data manipulation, email phishing attacks, insider attacks and (Serianu Limited, 2018). Other challenges that continue to plague this industry include advanced persistent threats (ATPs), Denial of Service (DoS) attacks, supply chain attacks, account takeovers, web application attacks and payment card skimming (Lockheed Martin Corporation, 2015).

On the global scene, various cases of data breaches have been reported within the financial sector over the past couple of years. A phishing attack on JP Morgan Chase and Co. in 2014 resulted in the exfiltration of information from 76 million households and 7 million small business. Even though there were no reports of any financial loss by bank officials, there was great concern that the stolen information could be used to launch future attacks on the affected customers. As a way of reducing the risk of similar attacks in future, Chase IT security staff decided to simulate a phishing attack to assess the preparedness and ability of their staff to respond appropriately (Henley, 2019).

In 2009, CheckFree Corp, an electronic bill payment service provider was adversely affected when hackers redirected their traffic to a malicious site. The result was that at least 5 million of their customers were duped into logging in to the fake site (Zhang, 2018). In 2016, Hackers installed malware on Bangladesh bank and stole credentials which they used to send requests for money transfer over a swift network to the Federal Reserve Bank of New York. The request contained instructions for the bank in New York to transfer funds to various recipients in Sri Lanka and the Philippines. This resulted in a loss of $81 million which was transferred by the bank to overseas accounts (Campanelli, 2018).

### *2.3.1 Data Breach*

Trend Micro (2018) describes a data breach as an incident where information is stolen or taken away from a system without the knowledge or authorisation of the owner of the system. The stolen data may include sensitive information such as credit card details, company trade secrets and matters of national security. According to OAIC (2018), A data breach occurs when personal/confidential information is subject to unauthorised access or disclosure, or loss. It can be caused by human error, deliberate malicious action or information system failure. Subsequently, data breaches also occur in scenarios where there is use of weak passwords, improperly configured systems, insecure uniform resource locators (URLs), poorly designed systems/applications and outdated systems. Some common examples of data breaches include theft of physical devices like laptops and external storage devices, unauthorised access to personal information, wrongful disclosure of information due to human error or negligence and unauthorised access to database records. Organisations and institutions whose personal data has been compromised can be adversely affected through financial loss and a damaged reputation. (Office of the Australian Information Commissioner(OAIC), 2018)

### *2.2.2 Abuse of Privilege Access*

According to Raytheon (2014), a privileged user is anyone that has elevated access to sensitive data, systems and computer assets. They are mostly associated with the organisations IT department and may include network administrators, database administrators or systems administrators. Account managers and corporate executives may in some cases be included among privileged users. Abuse of privilege access would therefor occur when privileged users take advantage of their elevated status to cause malicious damage to a system, steal information or leak the same to third parties. It can also occur through human error or negligence if privileged users do not use strong passwords for their accounts, do not store their credentials securely or if they click on a link that sent via a phishing email thus becoming susceptible to a malware attack that can allow cyber criminals to steal their credentials (Raytheon, 2014).

Privileged accounts are generally used within the IT infrastructure of most organisations for managing infrastructure or for enabling access between different applications. They are therefore required to maintain normal operations. On the flip side, they can be used by attackers to initiate and execute an attack against a company's infrastructure without being halted by existing security applications. Privileged accounts are therefore in a significant way responsible for the loss of data through exfiltration in a typical cyber-attack. One of the most commonly

referred to privilege abuse cases is the Edward Snowden leak in the year 2013. While working as a subcontractor for the National Intelligence Agency (NIA) in America, Snowden persuaded several of his colleagues to hand him their usernames and passwords arguing that he required the credentials to execute his job as a computer programmer. Using these credentials, he was able to gain elevated access to move laterally through the network and access restricted systems where he went ahead to exfiltrate classified information which he would go on to disclose to the public after going into exile. This would later be referred to as the most serious haemorrhaging of American secrets ever in the country's history of espionage (CyberSheath, 2014).

#### *2.3.4 Phishing*

Phishing is a type of social engineering attack where an attacker tries to retrieve sensitive or confidential information from a legitimate user. The attacker achieves this by pretending to be either an individual or an organisation that is trusted by the user. Information is sent via digital communication such as email from the attacker to the legitimate user with the sole aim of tricking them into sharing their personal and confidential data such as passwords or account credentials. Phishing attacks are normally classified into clone phishing, spear phishing and phone phishing. Clone phishing involves the cloning of contents from legitimate emails and resending these to unsuspecting recipients with the aim of tricking them to divulge sensitive information. Spear phishing attacks are targeted at a specific group of people who have something in common such as the employees of a specific organisation. Phone phishing is executed when an attacker sends text messages claiming to be from a legitimate organisation such a bank asking the recipient to change their password by clicking on a link or sending their account details (Saleem, 2012).

#### *2.3.6 Insider Attacks*

An insider attack is a malicious attack carried out against an organizations computer systems or IT infrastructure by an individual who has authorized access to critical systems, network resources or confidential data. Insider attacks which are also knowns as insider threats may be perpetrated by a current employee, former employee, consultant or even a board member. In actual sense, anyone who has access to insider information, confidential company data or access to IT systems must be considered as a potential threat. These individuals who pose a threat internally can be generally classified as the turn cloak, the pawn and the imposter. The turn cloak maybe an employee or contractor who is engaging in privileged access abuse. They use their elevated access rights to exfiltrate data. The pawn is just a normal employee who

makes a mistake that can be exploited by an attacker. It could be as simple as sending an email to the wrong recipient or forgetting to log out of their computer when taking a lunch break. The imposter is an outsider who manages to get access to a legitimate insiders' credentials with the aim of exfiltrating sensitive data that the insider is privy to (Petters, 2018). Figure 2.2 highlights the common behavioural indicators of an insider threat.

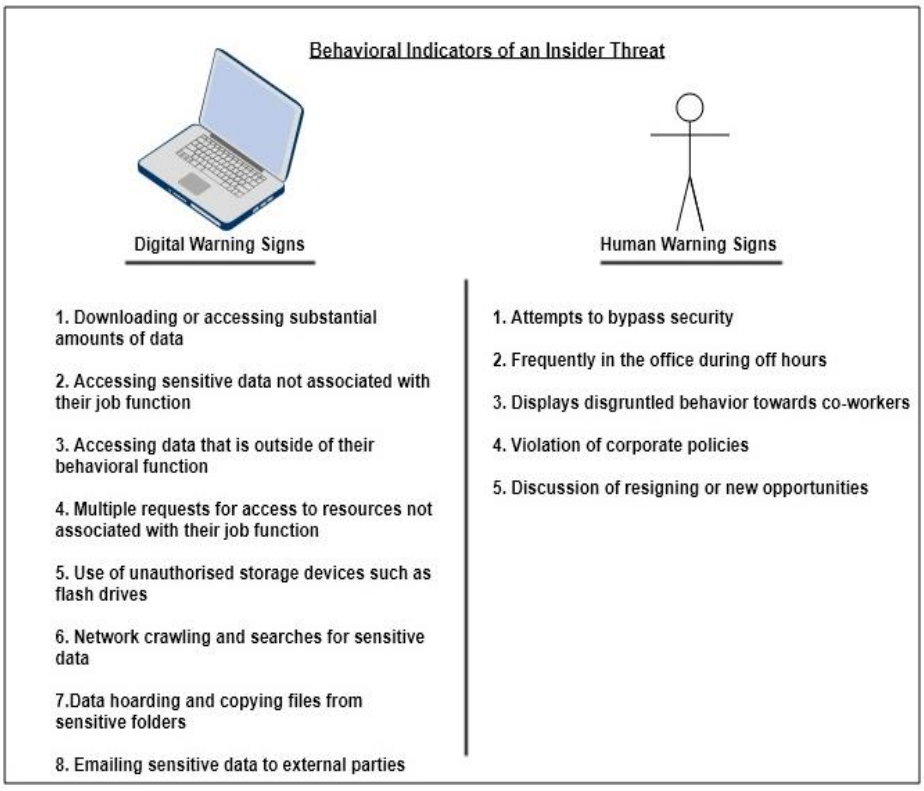



***Figure 2.2: Insider Threat Warning Signs, Source*** *(Petters, 2018)*

### 2.5 Understanding Social Engineering

According to Osterloo (2008), social engineering is defined as the successful or unsuccessful attempts to influence an individual/individuals into either revealing information or acting in a manner that would result in unauthorised access to, unauthorised use of, or unauthorised disclosure of an information system, a network or data. It is basically an art that is used by

attackers to manipulate legitimate users to divulge sensitive or critical information about an organisations data, systems or processes. Most cyber criminals will often use psychological tricks on an employee to deceive them and get critical information from them that would allow them to gain access into systems or sensitive records. Social engineering is therefore a non-technical approach of intrusion that relies heavily on human interaction and social skills. Though some few forms of it may involve use of technical skills (Oosterloo, 2008).

Social engineering attacks continue to enjoy a high success rate due to the natural human tendency to trust without questioning. Vasco (2015), highlights some of the most common forms of social engineering attacks such as email spoofing, man in the middle (MITM)attacks, instant messaging, covert redirect and website forgery. Companies in the financial sector seem to be heavily hit by such attacks as 21% of phishing attempts are targeted at getting customers financial credentials. In addition to this, phishing attempts are not easily detectable as 23% of email recipients read phishing messages and 11% go a step further to open the attached files (Vasco, 2015).

According to Pascu (2018), 8.5% of the total data breaches in the United States affected financial institutions in 2017. That same year experienced an increase in data breaches by 44.7% as financial services firms continue to fall victim to social engineering attacks 300 times more frequently than organisations in other sectors. In addition to this, organisations spent $7.35 million per breach on recovery costs (Pascu, 2018).

In early 2015, a cyber-crime ring known as Carbanak successfully exfiltrated funds from over 100 banks through a well-orchestrated spear phishing campaign that targeted administrators and bank clerks. This led to the installation of a custom malware known as Carberp which enabled them to impersonate the actions of their victims in order to send money out of the banks (SentinelOne, 2016).

In yet another incident, a conman managed to steal diamonds worth $28 million from a safety deposit box at the ABN AMRO bank in Belgium in 2007. The suspect who referred to himself as Carlos Hector Flomenbaum managed to gain the trust of the bank's employees for over a year by pretending to be a successful businessman. He befriended the bank workers and would even bring them a box of chocolates every time he visited the bank. One of the employees

eventually gave him access to the security deposit box which contained the diamonds which he made away with thus making this one of the biggest robberies committed by one person (Castle, 2007).

### 2.6 Forms of Social Engineering Attacks

According to Weippl (2014), social engineering attacks would usually involve physical, social and technical aspects at various stages of an attack. The physical approach involves the execution of physical actions with the aim of gathering information from a potential victim such as their date of birth, their pin number or login credentials. A good example of this is dumpster diving which involves searching or going through an organisations trash to retrieve information about them. The social approach relies heavily on social-psychological methods like manipulation and persuasion which are connected closely to the element of human trust. Technical approaches would often involve the use of software tools as well as the internet to harvest or gather information about an individual or company. Attackers would generally try to follow an organisation's digital foot print on various platforms such as their website and social media pages (Weippl, 2014).

#### *2.6.1 Dumpster Diving*

Dumpster diving is a social engineering attack that relies on the physical approach of going through a company's trash bin or dumpster with the aim of gathering useful information about the company, its employees or its customers. Some of the information that can be retrieved includes pieces of scrap paper with phone numbers or passwords written on them, details of employee's home addresses, list of customers, financial records and old company directories. This information may then be used by an attacker to prepare for an attack against the company in future (Gregg, 2006).

#### *2.6.2 Shoulder Surfing*

According to Rouse (2005), shoulder surfing refers to the use of direct observation techniques such as looking over someone's shoulder to get access to important information like their user name and password as they are typing on the screen or even their personal identification number (PIN) while they are accessing an automated teller machine (ATM). It can also be executed over long distances via vision enhancing devices like binoculars (Rouse, 2005).

#### *2.6.3 Google Hacking*

Google hacking is an information gathering technique used by an attacker leveraging advanced Google searching techniques. Google hacking can be used to identify security vulnerabilities

in web applications, gather information for corporate or individual targets, discover error messages, disclose sensitive information, discover files containing credentials and other sensitive data (Acunetix, 2019).

#### *2.6.4 Email Spoofing*

Email spoofing is a malicious activity where an attacker alters the original details of an email message to make it look like it has been sent form a legitimate source. Email spoofing is used by attackers to launch phishing attacks to trick the recipient into divulging confidential information that may give access to critical systems or company resources (Pandove, 2010).

### 2.7 Security techniques for Mitigation

Various approaches or techniques can be used for successful mitigation against social engineering attacks. According to Spinapolice (2011), the techniques for mitigation can be broken down into three categories. These categories are physical security, digital security and user awareness training (Spinapolice, 2011).

#### *2.7.1 Physical Security*

It goes without saying that physical security needs to be enforced throughout the organisation because any loophole can be exploited by attackers without much hesitation. All staff must be sensitised and made aware that the possibility of an attack is real. Various solutions can be implemented to prevent social engineering attacks that are executed using the physical approach. Installation of access control systems and use of photo identification badges within the building or office location can be useful in reducing the risk of piggybacking or tailgating attacks since it would ensure that no unauthorised persons can access the premises. In addition to this, surveillance cameras can be used to monitor movement in and out of the building thus deterring anyone with malicious intent to cause harm. Auto-locking doors fitted in areas with sensitive company resources or information would help to keep out unauthorised persons especially if a legitimate staff member forgets to close the door after leaving that area. It is also good practice to put up signs all over the office instructing employees not to plug-in flash drives or any other external storage devices that they may find lying around the premises. They should submit such devices to the relevant departments for further analysis. Any suspicious activity within the premises, irrespective of how minor it seems to be should be reported to security for further action. Additional physical security measures include alarm systems, motion detectors and physical security barriers (Hammoudeh, 2018).

To mitigate against dumpster diving attacks, organisations must ensure that they enforce effective policies for proper disposal of sensitive information. Devices such as cross-cut shredders should be deployed for shredding all documents before they are thrown into the trash bin. All digital media such as compact discs (CDs), hard drives and flash drives should be turned over to the IT department for appropriate destruction measures to be applied (Social Engineer, 2018).

With reference to shoulder surfing attacks, employees should avoid using their corporate laptops and mobile devices in public spaces that are crowded such as restaurants, airports and public transport vehicles. However, should they find it absolutely necessary to work while in public spaces, they should exercise extra vigilance and caution by being aware of their surroundings and where possible choose a sitting spot where their backs are against a wall to prevent prying eyes from observing what they are doing on their screens. Whereas the physically security measures are useful in keeping out the intruder, they are not effective enough in isolation to mitigate against online social engineering attacks which are propagated via digital means like phishing and spoofing (Cyberarms, 2010).

#### *2.7.2 Digital Security*

To mitigate against online social engineering attacks, a variety of tools and techniques are available. For man-in-the-middle attacks, organisations can discourage their employees form using public wi-fi networks while working on any office matter that is confidential. If it becomes necessary to work remotely, virtual private networks (VPNs) should be implemented to guarantee secure connections to office applications. In addition to this, all sensitive transactions should be secured via hyper-text transfer protocol secure (https) and two-factor authentications for all logins. Wi-Fi networks need to be separated into guest and office segments to ensure that outsiders cannot access any business applications. The use of intrusion prevention systems (IPS) can go a long way towards preventing unauthorised access to the network (Solid state systems, 2019).

With respect to email spoofing, organisations may make use of an email filtering solution such as a secure email gateway. Applications such as Mimecast and The Email Laundry can be useful for preventing spoofing attacks. Digital security measures may be limiting because they may fail to address attacks from within or insider threats from rogue employees or consultants (Hooper, 2018).

### *2.7.3 User Awareness Training*

According to Kumar (2018), information security user awareness training is an exercise that needs to be on going and must not exceed three months before reinforcement training is carried out. Various tools can be employed towards ensuring that employees are well equipped to detect and avoid social engineering attacks. Some organisations have gone ahead to make use of phishing simulation tools to train their employees on how to detect phishing emails. These tools provided by different vendors such as TrendMicro, Checkpoint and KnowB4 among others, play a critical role towards sensitizing employees to be keen when it comes to scrutinising emails for potential attacks. There are obvious advantages that organisations can realise from investing in phishing simulation solutions. These benefits include exposing those employees who are likely to fall prey to an actual phishing attack so that the organisation can take the necessary steps to train those that are considered the weaker links. A mock phishing test also gets employees talking about it thus keeping it top of their minds and as result they remain vigilant. On the other hand, these simulated attacks could be detrimental because they can disrupt normal flow of work within the office. If employees know that they are going to be tested, they may not take the exercise seriously thus dealing a huge blow to the whole initiative. Panicked employees may also cause a lot of disruption by flooding the IT help desk with calls regarding the mock phishing attacks (Stoy, 2018).

According to Osterloo (2008), there is a great need for organisations to employ various tactics and methods to counter social engineering attacks. They may choose to do this by countering these attacks as they occur or via structured implementation of security counter measures. To this end, Osterloo proposes the adoption of information security controls which include several ways of mitigating social engineering attacks. These controls are to be implemented from two dimensions, the function of the control and the controls according to the level within the organisation. With respect to the function of the control, organisations should consider implementing preventive, reductive, detective, repressive and corrective controls. Preventive measures can be implemented to stop an attack from happening. Reductive measures seek to minimize the damage that may accrue from an attack. Detective controls should be put in place to detect social engineering attacks as they occur as well as develop new preventive controls. Repressive controls are aimed at preventing a security incident from causing further damage while corrective controls are implemented to enable the organisation to recover from an attack. All this should culminate with an evaluation of why the attack happened, what caused it and

how it can be prevented in future. Figure 2.3 below shows the information security controls described above (Oosterloo, 2008).

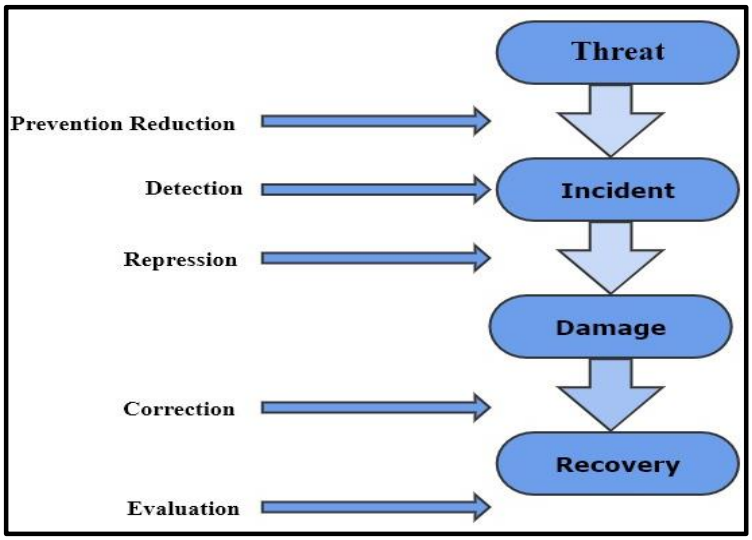



**Figure 2.3: Information Security Controls, Source** (Osterloo, 2008)

When it comes to implementing controls according to the level in the organization, Osterloo states that it is necessary to have strategic, operational and tactical controls in place. The strategic controls address the formulation of information security controls, standards and guidelines that would ensure business continuity in the event of an attack or breach. Tactical controls help to facilitate the implementation of security policies in the day to day business tasks while operational controls are concerned with the implementation of technical and non-technical safeguards. The limitation with Osterloo's proposed method of countering social engineering attacks is that these measures in isolation cannot stop social engineering attacks. Controls may be in place, but the human factor is still not covered. Awareness on social engineering tactics is not given much weight in his proposed framework (Osterloo, 2008).

As another way of countering social engineering attacks, Gardner and Thomas (2014) propose the implementation of the Social Engineering Defence Framework which consists of four essential phases. In the first phase, the organisation determines their exposure to social engineering attacks by looking at their sites and resources in the same manner as a social engineering attacker. The second phase involves the evaluation of the defence mechanisms in

place by analysing employee's resistance and reaction to simulated attacks. The third phase is all about awareness and is executed by teaching employees how various attacks are executed and what damage they can cause to the organisation. In the fourth and final stage, the organisation focuses on streamlining the existing technologies, policies and information security measures. The limitation with this framework is that it does not propose any way of evaluating employee's knowledge of social engineering attacks. It may have an element of carrying out simulated attacks but that alone is not enough to assess employee's awareness for most forms of social engineering attacks. Figure 2.4 below helps gives an illustration of the SEDF framework (Thomas, 2014).

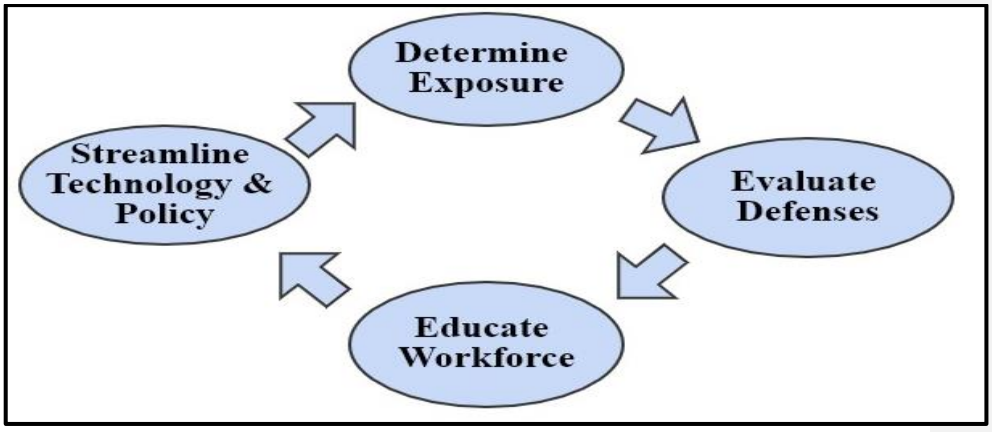



***Figure 2.4: Social Engineering Defence Framework, Source*** *(Thomas, 2014)*

## 2.8 Existing Tools for countering Social Engineering Attacks

There are various automated tools currently available in the market for countering social engineering attacks. This study explored some of those tools by looking at how they work to counter attacks as well as their pros and cons. The tools considered were Phish Insight, Phish Me, Phish Threat, Phishing Box and KnowB4.

### *2.8.1 KnowB4*

KnowB4 is a well-known security awareness training and simulated phishing platform developed and sold by the KnowB4 company whose headquarters are based in the United States of America. The platform gives IT teams the ability to conduct security awareness trainings that are integrated with mock attacks, web-based training and regular assessment via simulated phishing attacks. Employees are taken through a series of training modules before being subjected to these mock attacks. The platform has its various benefits and limitations.

Some of its benefits include the fact that it has a user friendly and intuitive interface that makes it easy for employees and IT teams to interact with. It gives users access to a large security awareness training library and its mock phishing templates are available in 24 languages thus ensuring a wider global reach. Apart from training users and raising awareness, the simulated phishing attacks give them the ability to know how to react and respond to real life attack scenario. However, despite its effectiveness, the KnowB4 platform simulated attacks are more focused on training users about how to identify and respond to phishing attacks. The platform does not address how employees should respond to attacks that do not require any technical expertise to such as tailgating, piggy backing, shoulder surfing and dumpster diving. The tool therefore assumes that the only attacks to be concerned about are the ones propagated via email which is not the case (KnowB4, 2019).

#### *2.8.2 Phish Insight*

Phish Insight is a product from Trend Micro, a security firm based in the Unites States of America (U.S.A). This product or tool enables organisations to counter online social engineering scams by educating its employees about how to recognise and avoid email phishing attacks. The tool also provides a platform for testing employee awareness via simulated phishing attacks. These simulated attacks help to gauge their employee's reaction and responsiveness to such attacks thus identifying their areas of weakness which would require further training or retraining. The major benefit of using Phish Insight is that it gives organisations various options to select from with the standard and starter packages which are free for a specified number of users versus the premium package which has no limit on the number of users form a licensing perspective. This ensures that organisations with a tight budget can choose the option that works for them without bursting their budget. The platform also makes it easy to conduct a phishing simulation because it can be carried out in four simple steps which takes about five minutes to execute. Despite the above advantages, this platform is purely limited to training and testing users on how well they can respond to online attacks propagated via phishing techniques. It does not make any effort to address other forms of social engineering attacks especially those that affect physical security (Trend Micro, 2019).

#### *2.8.3 Phish Threat*

Phish Threat is a phishing simulation tool from Sophos, a company based in the United States of America (U.S.A) that provides security solutions for various organisations globally. Phish Threat works by creating and subjecting users to simulated phishing attacks. The product also provides a wide training platform on the latest phishing techniques which ensures that end user

training is covered holistically with scenarios ranging from beginner to expert levels. The product is beneficial because it integrates the testing and training phases into very simple to use modules that can be administered to users on the spot. The training platform is also available in nine languages making accessible to users globally. The results from the phishing mock tests are bundled up in comprehensive reports which reveal the users or employees who are most prone to a phishing attack (Sophos, 2019). The major limitation of this product it also focuses primarily on addressing online social engineering attacks in the form of email phishing scams. It does not have any reference whatsoever as to how physical forms of social engineering attacks can be countered by the user (Sophos, 2019).

#### *2.8.4 PhishMe*

PhishMe is another product in the market that is used to counter online social engineering attacks. The product is from a security company called Confense based in the United States of America (U.S.A). The product works by using the latest tricks and techniques being employed in real life phishing attacks. This gives users the ability to recognise as well as report email phishing scams. PhishMe provides boardroom-level reporting for executive teams which showcases the results of the simulated phishing attacks.The product is a great asset to organisations as it integrates the use of the Confense Reporter application which enables users to spot and report suspected email phishing attempts. Another benefit for organisations is that the product is available as both a free and a paid for package. The Free package can serve organisations who have a tight security budget. As is the case with all the other three tools that have been considered, PhishMe is limited by the fact that it does not have the ability to train and test a user's awareness about physical forms of social engineering attacks. The tool is primarily focused on creating awareness on phishing attacks and how users can respond to them (Confense, 2019).

### 2.9 Conceptual Framework

To address the continuous threat posed by social engineering attacks against the financial sector, this study led to the development of a web-based cybersecurity awareness and assessment tool. This tool can enable organisations to assess the cyber strength and/or cyber preparedness of their employees by subjecting them to an assessment that spans across various cyber security topical areas like phishing, physical security, internet browsing, social networking, social engineering scams, proper use of mobile devices and mobile apps. Organisations can use it to gauge their employees' level of understanding about social engineering attacks as well as overall information security awareness and as a result reduce

their level of vulnerability to attacks. The results from the assessment will are used to cluster employees into different categories based on their performance.

The employees who perform poorly in the tests are scheduled for further training in their identified areas of weakness, whereas those who perform well are rewarded by the organisation as a way of giving the rest an incentive to work hard at getting a better result the next time they take the test. The report generated from the assessment can be used to help organisations identify the areas that they are most vulnerable and what they need to do to get rid of the security gaps or weaknesses. The assessment report also shows all employees who have completed the test and those who have not. This can be useful for the human resources department as organisations may want to integrate this with their performance appraisal exercise. All employees who do not complete this report receive a negative review form their supervisors. This would serve to ensure that all staff take the exercise seriously.

As compared to other automated social engineering mitigation tools, the main benefits that this tool provides over other techniques of mitigation for social engineering attacks is that it goes beyond the normal scope of common simulation attacks to get a broader understanding of employee's knowledge levels. It also allows for the creation of custom questions that are specific to an organisations policy, culture, weaknesses or any other area that they may want to cover. Organisations can now cover more ground as they assess their people's knowledge on all areas at one go rather than having to do separate training sessions for physical security, digital security, simulated phishing attacks and general awareness. This helps them realise a lot of savings on time needed to train as well as the overall cost of training because more focus is allocated to specific areas of weakness. Figure 2.4 compares the abilities that current tools with the cyber prep assessment tool.

| Focus Area / Name of Tool | Assess employee ability to counter email phishing attacks | Assess employee ability to counter physical forms of social engineering threats | Assess employee ability to properly manage their passwords | Assess employee knowledge on safe web browsing practices | Assess employee knowledge level of insider threats and how to counter them | Assess employee general preparedness through a test assessment platform |
|---|---|---|---|---|---|---|
| **Cyber Prep App** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **KnowB4** | ✓ | X | X | X | X | X |
| **PhishMe** | ✓ | X | X | X | X | X |
| **PhishMe** | ✓ | X | X | X | X | X |
| **Phish Threat** | ✓ | X | X | X | X | X |
| **Phish Insight** | ✓ | X | X | X | X | X |

***Figure 2.4: Cyber Prep vs other tools***

Figure 2.5 gives an outline of how the proposed assessment tool works. This consist of three stages namely the input, processes and output. The input that the systems receives is the answers to the assessment questions when an employee takes the test. The processes of the system are mainly analysing and scoring the tests submitted by the employee to generate a detailed report of the test results. These results are then stored in a repository. The output generated by the system is in form of performance reports and recommendations for the employee which are largely dependent on their performance.

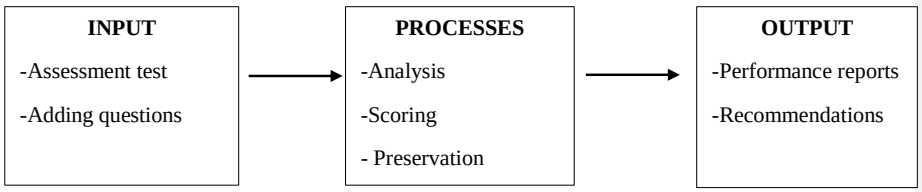



***Figure 2.5: Conceptual Framework Diagram***

# Chapter 3: Methodology

## 3.1 Introduction

This chapter introduces the methodology that was used to develop the web-based cybersecurity assessment tool for testing employee's level of preparedness and responsiveness against social engineering attacks. It also focuses on the design as well as implementation process.

## 3.2 Methodology

The methodology that was used to design, develop and test the web-based assessment tool is the Rapid Application Development (RAD) methodology. According to Korkishko (2017), RAD is a condensed software development model that is used to produce high quality software products at very low costs. It is suitable for cases where development time is minimal or limited. It distributes the development phases of designing, building and testing into short, iterative cycles. The major benefit of the RAD model is that it makes the whole development process effortless and encouragers feedback from the end users for improvement (Korkishko, 2017).

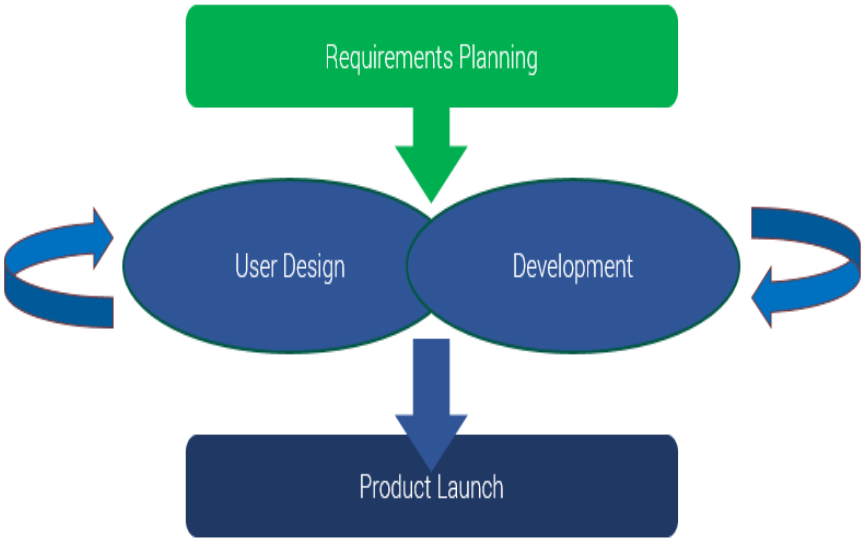



**Figure 3.1: The stages of a RAD Model, *Source*** *(The App Solutions, 2018)*

### *3.3.1 Requirements Planning and Analysis*

This phase involved a discussion with various stakeholders through a series of workshops to determine the current systems that were in place. This was followed by the definition of the requirements (including hardware and software) for the web-based assessment tool. The objectives and the scope were clearly defined at this stage. This included tasks such as identifying the relevant assessment questions to be included within the application as well as a clear description of the objectives that the assessment tool would achieve. The project team prepared documentation that would capture the scope of the proposed assessment tool as well as the associated costs for developing it and the expected duration of the project.

This study employed the use of various data collection methods to gather information about what kind of data would be consumed by the system. The observation method was used to determine the behaviour of employees within the financial sector the results were captured so they could be used to design the assessment questions for the system. Interviews were conducted with various employees within the financial sector to determine the various of social engineering threats they have been exposed to and this proved useful in addressing the first objective of this study together with the literature review that was carried out in chapter 2. The literature review identified the common forms of social engineering attacks in the financial sector as well as existing solutions for mitigating against such attacks. Online surveys were used during the system testing phase in order to determine the effectiveness of the system especially during the user acceptance testing phase.

### *3.2.3 User Design*

The design phase involved analysis of the data that was collected from various key stakeholders to determine how it would be consumed by the system. The project team also developed the system structure in line with its expected functionality as well as development of the screen layouts. Various tools such as sequence diagrams, use case diagrams, context diagrams and entity relationship diagrams were used to come up with the design of the system. The expected deliverables from this phase include a detailed system area model and an implementation plan. After finalising on the system design, the project team sought the approval of the project owners before proceeding to the next phase.

### *3.2.4 System Development*

At this stage, the final system design was used to create and test the various components of the proposed assessment tool. This included the graphical user interface as well as coding of the various functionalities as per the specified requirements. The coding of the various models was

carried via the PHP platform. The identified assessment questions as well as the various categories were designed and entered into the system library. After generating the test data, the system was presented to various stakeholders for testing and retesting in order to identify any weaknesses or gaps. Plans and procedures for going live as well as user training materials were also developed at this stage.

#### *3.2.5 Testing*

The system was subject to a wide range of tests in order to determine its effectiveness and whether it met the overall expectations as per the established requirements. The tests conducted were unit tests, integration tests, system tests and user acceptance tests. The unit tests were used to determined if the different modules had been properly coded. The integration tests how the various modules interacted as a block upon integration. The user acceptance tests were critical in order to determine whether the overall system had met it's objective with reference to user friendliness, robustness and response time

#### *3.2.6 Validation*

The test results were captured via questionnaires circulated to the various test groups. This was useful in determining whether the system serves the purpose for which it was designed and if it has met the overall objective of the study.

#### *3.2.7 Product Launch*

This was the final stage where the system was prepared to go live. The project team conducted user training as they carefully followed the detailed plan designed at the development stage. This was then be followed by the launching of the application. The performance of the new system was monitored and reviewed to identify any bugs or weaknesses that needed to be rectified. Once the system was declared stable, the project team officially handed over the system to the project owners.

# Chapter 4: System Design and Architecture

## 4.1 Introduction

This chapter discusses in great depth how the analysis and design phases were executed. It gives a broader picture of the functional and non-functional requirements that were identified during the analysis stage. In addition to this, the architecture of the proposed system is explained by expounding further on the conceptual framework. The architecture reveals various facts about the system such as the its input, output, processes and network design.

## 4.2 Requirements Analysis

### *4.2.1 Functional Requirements*

The functional requirements for the system were identified as follows:

1. **Generation of assessment questions**
   After determining which department an employee belongs to, the system generates the questions from the system library and displays them on the screen.
2. **Test administration**
   The system accepts user input in form of answers to the questions.
3. **Scoring of answers**
   The system analyses and scores the answers using a predetermined answer sheet.
4. **Report Generation**
   The system also generates a report of on the user's performance together with recommendations on further steps to be taken as well as identification of areas of vulnerability.

### *4.2.2 Non-Functional Requirements*

The properties and constraints of the system are specified by its non-functional requirements.

i. The system should be easy to use and have a simple user interface.
ii. The system should allow users to login securely.
iii. The system should be able to accurately analyse and score answers submitted by users.
iv. The system validates user's credentials when they are logging in.

### 4.3 System Architecture

The system comprises of various phases which are vital for its proper functioning. The employee is authenticated by the system which also checks the department they belong to. The department determines the level and type of assessment test to be administered to the employee. The systems redirects the employee to the test page where they can choose to take they test by clicking on a button. Upon completion of test, the employee submits the answers for scoring. The scoring and analysis component of the system checks the answers submitted against pre-defined answer sheets stored in the database and evaluates the user performance based on the results produced to determine what classification to give an employee based on their performance and whether they are above or below the threshold. The report component of the system generates a full report of an employee's performance and gives recommendations on what further steps need to be taken. Figure 4.1 depicts how the system is designed to function.

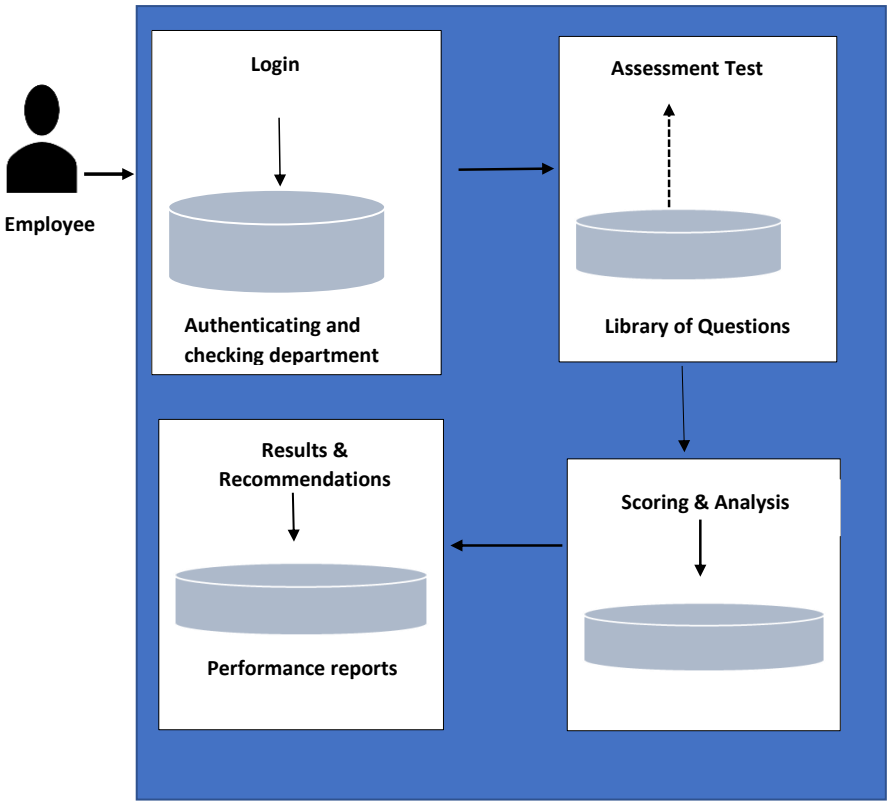



*Figure 4.1: System Architecture*

#### *4.3.1 Input*

The system receives input from an administrator who has rights to create or remove user profiles. The administrator also uploads the specific assessment questions for the employees. Finally, the administrator sends a notification to all employees alerting them when it's time to take the test.

The system is also designed to receive input from the employees who give their credentials via a logon screen for the web-based system. Upon authentication, the employee then goes ahead to take the test by clicking on the link sent to them by the administrator and selecting appropriate answers to the questions from the multiple choices given before submitting the test for scoring.

#### *4.3.2 Processes*

Upon receiving input from the employees, the system randomly generates the sets of questions based on the job level of the employee as well as the employee's previous performance. If the employee has privileged access to the organisation systems, then questions with greater level of complexity would be generated compared to an employee with low level access. Additionally, if an employee scored poorly in the previous assessment then the questions generated would focus on their area of weakness. A candidate is categorised as having performed poorly if they receive a score of 50 points and below. A candidate who scores between 51 and 70 points is categorised as having passed the test but still requiring further training in specific areas whereas a candidate with a score of 71 to 100 pints is deemed to have performed exceptionally well with just a little bit of training required to bridge any existing gaps. The scoring of answers is executed by matching the answers provided by the candidate with the answer sheet in the database. The system then analyses the results by sing already predefined parameters before allocating a grade to each candidate together with the associated recommendation.

#### *4.3.3 Output*

Upon completion of the analysis and scoring process, the system generates a detailed report of each employee's score or grade as well as the recommended action to be taken. The recommended action for a candidate who scores poorly is for them to undergo training in various programs before retaking the same test again within a period of not more than three months from the date of the previous test. The system also provides a report on the areas of weakness or vulnerability that need to be addressed by the organisation in question.

### 4.4 System Design Tools

Various design tools were used by the project team to come up a detailed conceptual framework of the system. The team implemented the use of use case diagrams, context diagrams, sequence diagrams and entity relationship diagrams (ERDs).

#### *4.4.2 Context Diagram*

The project team implemented the use of a context diagram to show how information flowed between different processes in the system. This was important because it represented how different functions or processes would capture, manipulate, store and distribute data between the system and its environment as well as between the different components of the system. The diagram in figure 4.2 explains how the different external entities interact with the internal entities of the system. The administrator sends a login request by keying in his credentials which are checked against a matching record on the database. The system authenticates the administrator allowing him to continue accessing other resources. The administrator creates user profiles on the system which are stored in the database. Test questions are uploaded into the system library and a test notification is sent to all employees. The employee sends a login request and after authentication proceeds to take the test. The submitted test is analysed and scored by the system and a detailed report is then generated and store in the database. This is well represented in figure 4.2.

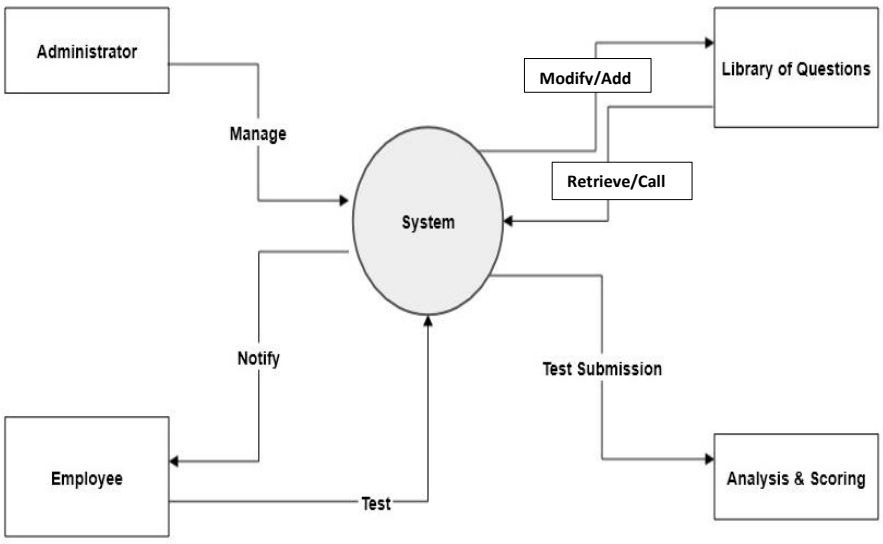



***Figure 4.2: Context Diagram***

### *4.4.1 Use Case Diagram*

The interaction between the employees and the web-based assessment tool is depicted as shown in figure 4.3 below.

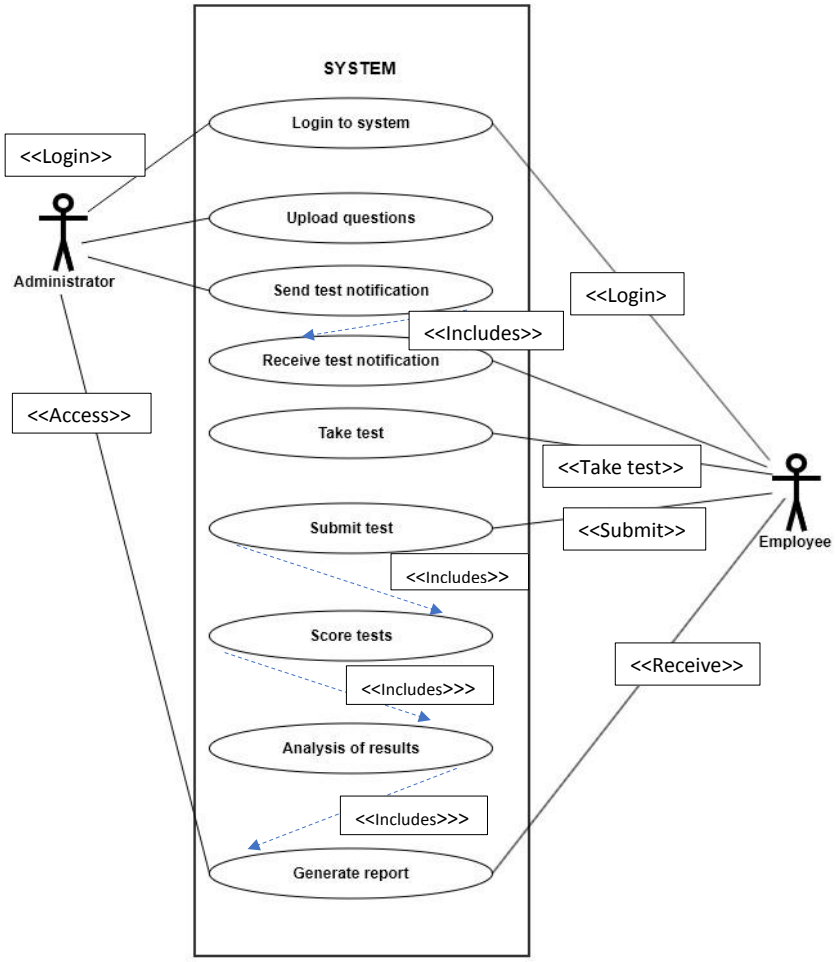



**Figure 4.3: Use Case Diagram**

In figure 4.3 above, the use case is employees participating in an assessment test to determine their level of preparedness against social engineering attacks. The actors in this case are the employees and the super admin. The employees provide input by login in to the web-based assessment tool using the credentials supplied to them by the super admin, they take the

assessment test and finally they submit their responses for processing by the system. The super admin provides his input by creating user profiles and designing or customising the questions to be included in the assessment.

### *4.4.3 Sequence Diagrams*

The project team made use of sequence diagrams to depict the interaction between the objects in the system in a sequential order. This was important because it showed how and in what order the components of the system would function. The system is designed to accept input from both the user and administrator. The administrator accesses the system after logging with elevated user privileges. The system checks the user's credentials against what is stored in the database before authentication can happen. If the credentials provided match what is in the database, the administrator is authenticated. However, when the credentials do not match, an error message is displayed on the screen indicating that the credentials supplied are not valid. The administrator is then able to create or delete user profiles where necessary. When a new user profile is created, the details are captured in the system's database on a table called 'user_Profiles. The administrator also creates the different subject categories and their related questions which are stored on a table known as 'test_Questions'. The administrator then sends a notification to all employees who are required to take the test.

The system also accepts and authenticates standard user login requests which are validated after being checked against the 'user_Profiles' table. The system is prompted to generate the assessment questions when the user submits a request to take the assessment based on the notification sent by the administrator. The user takes the test by selecting the appropriate answer from the list of multiple-choice options and then submits the answers.

The system carefully analyses and scores the answers submitted by the user by referring to the pre-defined answers stored under the 'answer_Sheet' table. A report on the user's performance is generated by a system notification which is sent to the administrator and the user. The report is also stored in database under the 'performance_Report' table. Figure 4.4 expounds more on this.

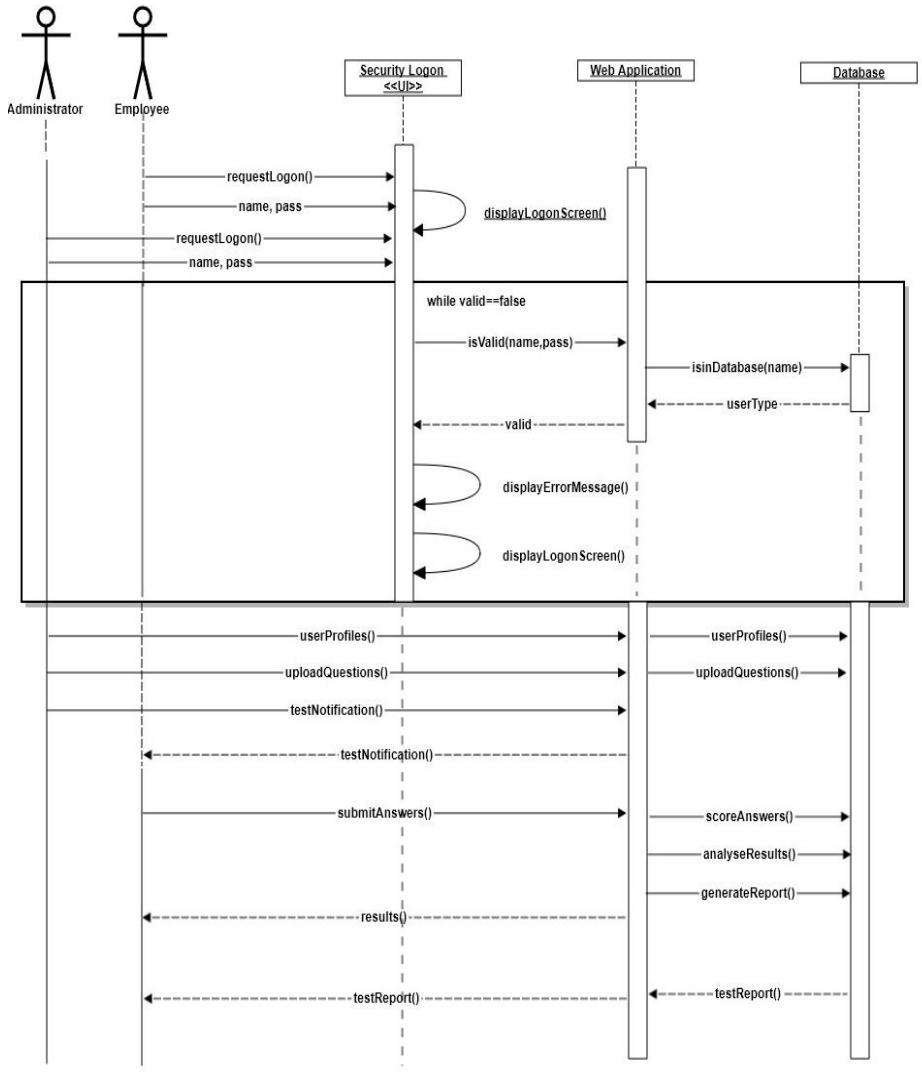



**Figure 4.4: Sequence Diagram**

### *4.4.4 Entity relationship Diagram*

In order to come up with the design of the system database, the project team implement the use of an entity relationship diagram (ERD) to show the relationship between the different entities in the database. Figure 4.5 represents this in further detail.

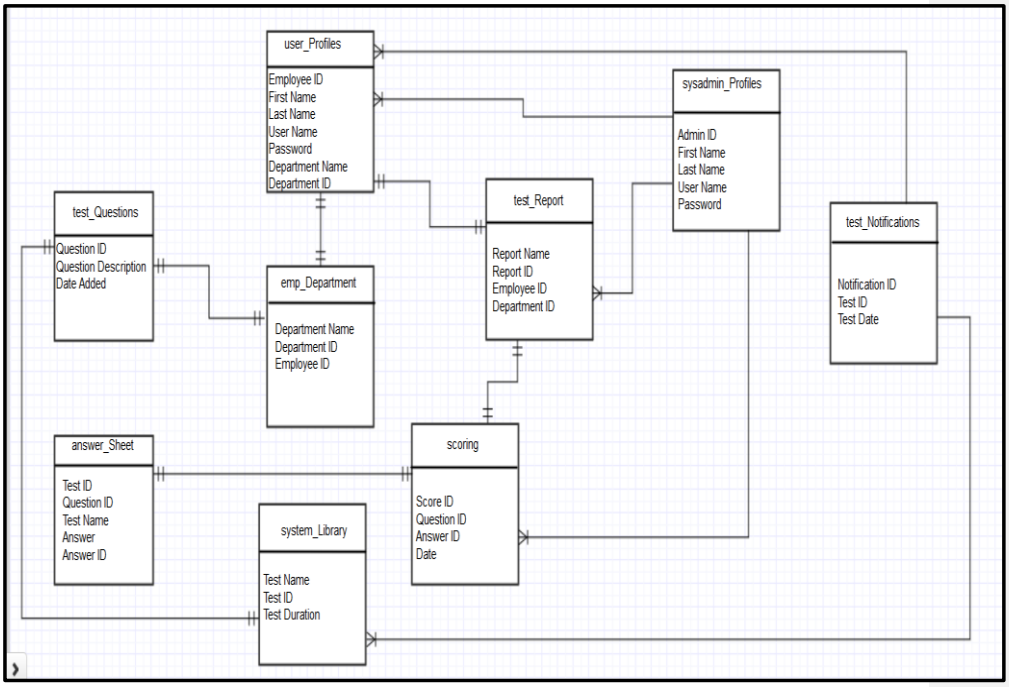



***Figure 4.5: Entity Relationship Diagram***

### 4.5 Security Design

The Secure Socket Layer (SSL) protocol was implemented in the design of the system to guarantee confidentiality of the information being relayed between the client and the server. To achieve this, the dedicated host for the web application was assigned a specific IP address and an SSL certificate was purchased and set up so that the web application site could use https instead of http which provides for more security. The SSL certificate encrypts all information flowing to and from the host of the web application.

The system was also designed to lockout users after three unsuccessful login attempts. In addition to this, symmetric encryption of the data was used to ensure that the integrity and confidentiality of communication and messages between the client and the server maintained. This was achieved by ensuring that the all information relayed from the client to the server is encrypted using a secret key.

### 4.6 Wire Frames

The project team used the Wireframe Pro tool to develop a schematic blueprint to give a visual guide representing the skeletal framework of the assessment tool. This exercise was crucial because it provided a layout of how the different elements or components of the system would be arranged. It also provided a rough estimate of their size. Figures 4.8 to 4.12 give a visual representation of the layout and arrangement of the screens.

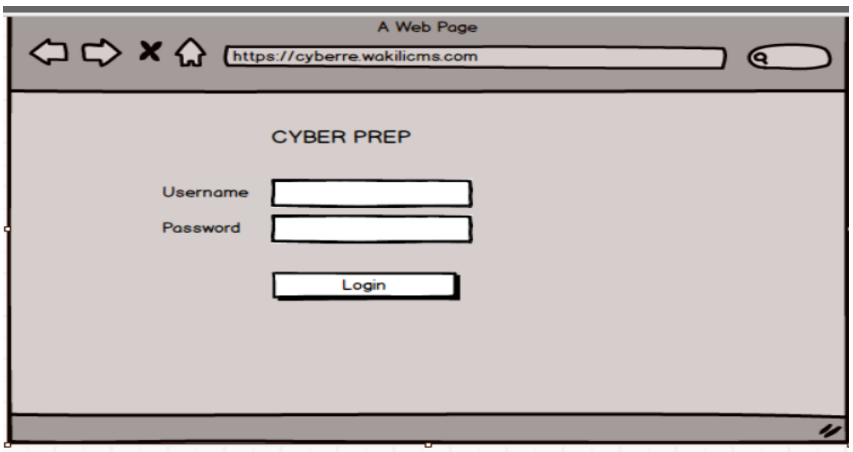



***Figure 4.8: Login Screen***

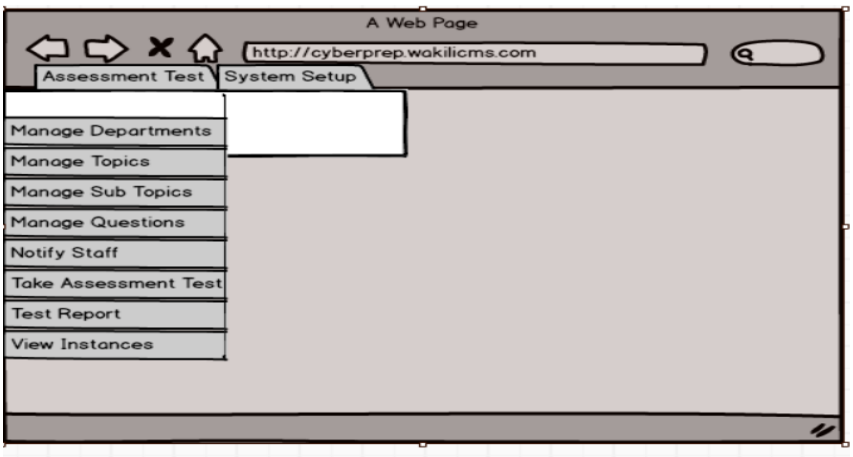



***Figure 4.9: Welcome Page***

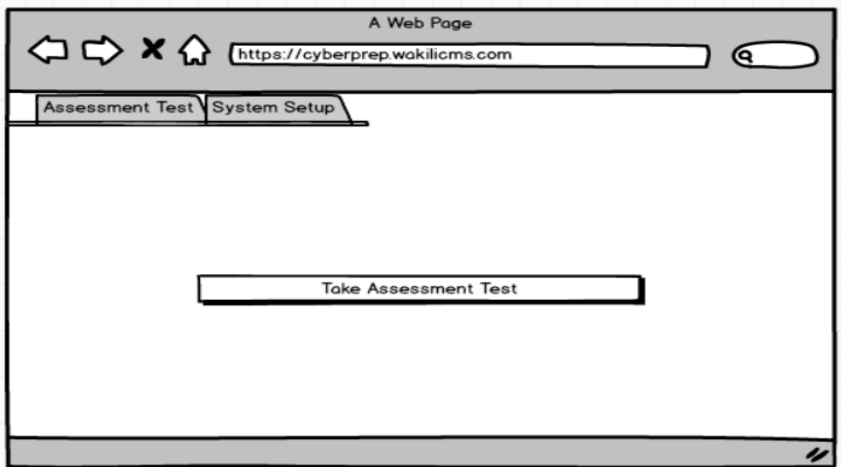



*Figure 4.10: Beginning the test*

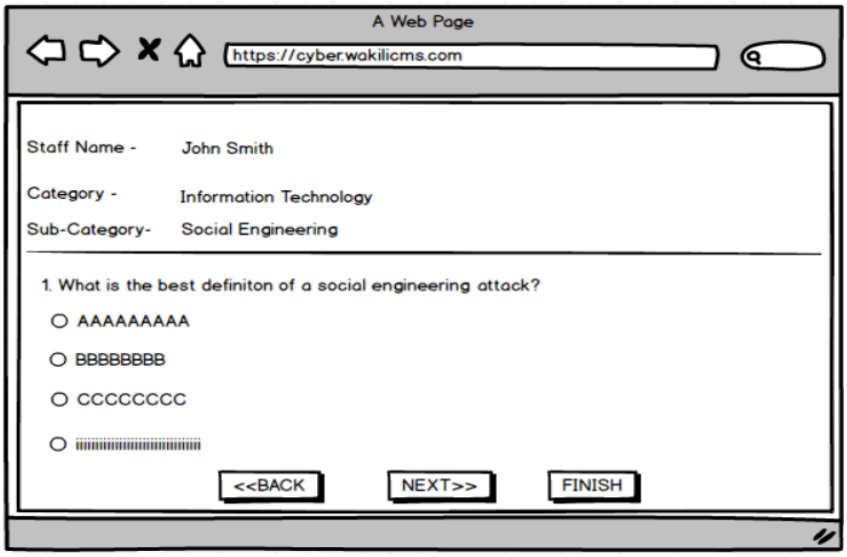



*Figure 4.11: Assessment Page*

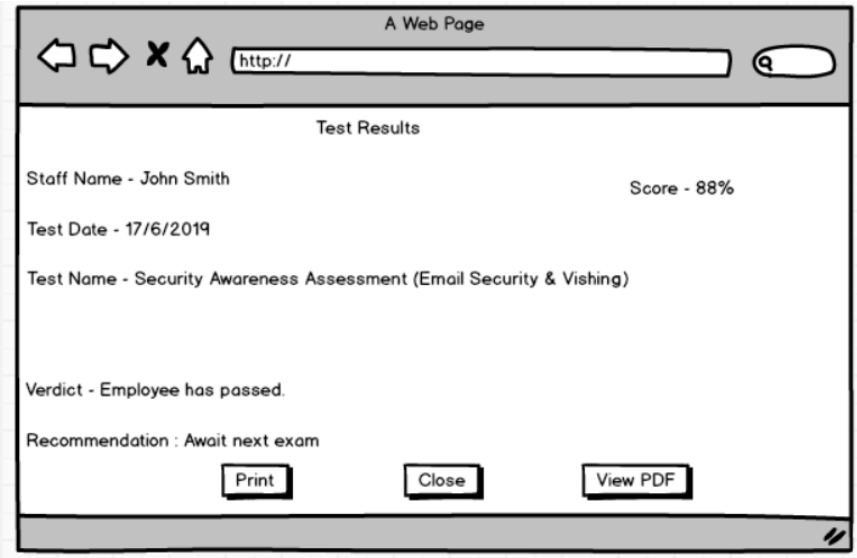



***Figure 4.12: Test Results***

# Chapter 5: System Implementation and Testing

## 5.1 Introduction

This chapter discusses the how the development of the assessment tool was carried out. It highlights the development environment that was used by the project team as well as the hardware and software requirements that were considered. The chapter also looks at the various features of the system and the approach that was used to carry out system testing.

## 5.2 Development Environment

### *5.2.1 Hardware Requirements*

The minimum hardware requirements identified for the system to function effectively are as follows:

i. **Application Server**

The server hosting the system requires a hard disk of 2 terabyte (2TB) which is enough to host the database which contains employee profiles, the library of questions as well as the reports generated after each test. The hard disk will also be enough to accommodate a daily backup of the server. The memory allocation is sixteen gigabytes (16GB) of random-access memory (RAM) to ensure that the system performs to its optimum even when there is a heavy load of users. A processor of 3.5 gigahertz (Ghz) allows the system to respond quickly to user requests as well as perform other critical system operations.

ii. **Client Workstation**

The client workstation or computer requires a minimum hard disk space of five hundred gigabytes (500GB) for the optimal functioning of the operating system. For optimal user experience while loading pages from the application server, a minimum RAM capacity of eight gigabytes (8GB) is not only desirable but necessary as well as processing speeds of not less than 2.8 gigahertz.

iii. **Certificate Authority**

The certificate authority server is required to generate the private and public key certificates that would be used to secure the communication between the server and client workstations thus ensuring confidentiality and integrity of the information being transmitted.

**iv. Cisco Network Switches**

Network switches are required to relay and direct network traffic between the server and the client workstations.

### *5.2.2 Software Requirements*

The minimum software requirements were identified as follows:

**i. Coding language**

The system is web based and therefore the preferred language of choice that was identified for developing the system was Hypertext Preprocessor or PHP version 3.5.2. PHP was used by the development team to code the different modules of the entire system and also to integrate them. The system was broken down into different units and each unit assigned to a team to ensure that the development process was executed without a delay. The various components included the login screen, the welcome page, the test assessment component, the scoring and analysis module, the performance reporting component and the database. All these were assigned to a specific team which was responsible for scripting the respective code.

**ii. Server operating system**

The operating system selected as the preferred option to host the system is Windows Server 2016 Standard.

**iii. Client operating system**

The preferred operating system was Windows 10 Professional for the client workstations.

**iv. Database**

The database platform selected is MySQL 5.5.25a. MySQL statements were used to create the various tables within the relational database. The tables created include user profiles, performance report, test questions, system library, system admin profiles, scoring, answer sheet and test notification. For the design of the test questions, the project team used the list of common social engineering threats identified in chapter 2 to develop the questions.

v. **Web browser**

The System is guaranteed to work with any of the common web browsers which include Mozilla Firefox, Google Chrome and Microsoft Edge for the client workstations.

Commented [BI1]: For server or client?

Which versions were these?

vi. **Web Server**

The web server version that was implemented is Apache 2.4.2

vii. **Network Requirements**

The system should be deployed over a network with speeds ranging between 100 megabytes per second (MBPS) and 1000 megabytes per second (MBPS) for ethernet networks and the 802.11 standard for Wireless Fidelity (WiFi) which provides for speeds of up to 3200 megabytes per second (MBPS) to facilitate or support up to 250 client computers.

### *5.2.3 Security Requirements*

The project team identified the following as the minimum requirements for security of the system:

i. **Secure Socket Layer (SSL)**

The project team opted to implemented SSL via the Microsoft Internet Information Services (IIS)feature. The certificate was requested and installed on the web application server to guarantee secure communication between the clients and the application server.

ii. **Public Key Infrastructure (PKI)**

The Public Key Infrastructure was implemented using the Windows Active Directory Certificate Services feature which allows the creation and management of public key certificates within a local network. This set up ensured that all information and communication relayed between the client and server is encrypted thus guaranteeing confidentiality and integrity.

iii. **Account lockout**

The system was designed to lock a user's account after three unsuccessful login attempts.

### 5.3 Dataset

The data collected in chapter 3 was used to generate the assessment questions based on the observations made about the behaviour of employees in the workplace when it comes to responding to social engineering threats. From the literature that was reviewed in Chapter 2, it was possible to construct relevant questions for the different categories of their employees based on their competency and risk levels. Other forms of data such as the names of the employees, their departments and roles were also considered at this point.

### 5.4 Loading the dataset

Once all the relevant assessment questions had been constructed, they were loaded into the system library repository where they can be accessed by the system and presented via a graphical user interface to the users. The answers to the respective assessment questions were also loaded into an answer sheet table as per the entity relationship diagram in Chapter 4. The user profiles of all employees together with relevant details of their roles were also uploaded to the user profiles and employee department tables.

### 5.5 Algorithms

The development of the system relied on the conceptual framework in chapter 2 of this study. The system was designed to observe the following rules or algorithms. When an employee logs in, the system checks the user credentials against what is stored in the 'user_Profiles' table. The user attributes that the system relies on here are the username and password. If the credentials provided match what is stored in the table then the employee is granted access to the system. However, if there is no match then the system returns an error indicating that the wrong username or password has been entered. If the wrong password is entered more than three times, the system will automatically lock out the user. This rule was thus be represented as follows:

***If username is "" and Password is ""***
***Then grant access***
***Else Print error "Your username or password is incorrect"***
***End***

Upon successful logon, the system then checks which department an employee belongs to by referring to the 'emp_Department' table for the department name, department id and user id attributes. Depending on which department the employee belongs to, the system selects the most appropriate exam to administer to the employee. This shows how the rule in the first

decision component from the conceptual framework in chapter 2 was applied. When an employee clicks on the 'take assessment test' button, the appropriate assessment test is loaded from the 'system_Library' table by referring to the test name and test id attributes. This was achieved by defining a rule as follows:

***If employee belongs to accounts department***
***Then administer test number 2***
***Else if user belongs to IT department***
***Then administer test number 1***
***End***

Once the employee completes the test and submits it for scoring the system analyses the questions using the answers from the 'answer_Sheet' table using the test id, question id and answer id attributes. This is then followed by the scoring process which is captured in the 'scoring table' where the employee is graded according to their performance. A report of the employees' performance is captured in the 'test-Report' table. Depending on a user's performance, the system takes a decision to either fail the student and recommend a resit or pass the student and recommend that they sit for the next assessment test. This demonstrates clearly how the rule for the second decision component in the conceptual framework in chapter was applied. The system has a set thresh hold of 70 points as the pass mark. The rle that was used to represent this was as follows:

***If employee score is > 70***
***Then then give a pass and recommend employee for next test***
***Else give a fail grade and recommend a resit***
***End***

The system administrator can modify or add assessment questions to the 'system_Library' and can also view the various employee performance reports from the 'test_Report' table.

**5.5 System Features**

The system is accessed via a local uniform resource locater (URL) that redirects the user to a logon screen as depicted by figure 5.1 below.

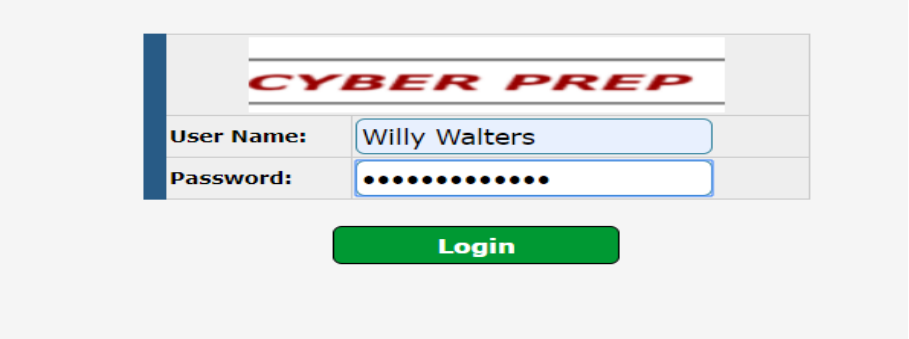



*Figure 5.1: Logon Screen*

Upon successfully login into the system, the user is redirected to the assessment page from where they can choose to start the assessment by clicking on the "Take Test" button shown on figure 5.2. The first rule for the first decision component in the conceptual framework found in chapter 2 of this study was implemented at this point. The system checks which department the employee belongs to during the logon process before selecting the appropriate assessment test to be administered. For instance, if the employee belongs to the finance division, then the assessment test that is designed for users within that department is made available to the employee.

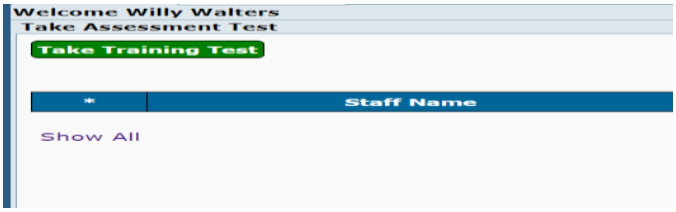



*Figure 5.2: Start Test*

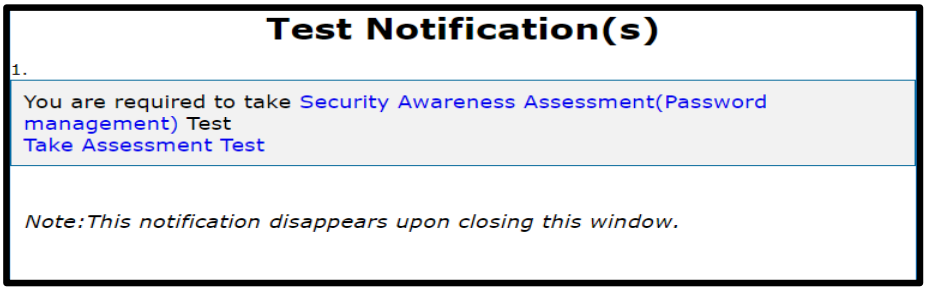



*Figure 5.3: Link to Assessment Test*

When the user clicks on the "Take Assessment Test" link shown in figure 5.3 above, they are redirected to the page that has the assessment questions and once they select the appropriate category and group, they can begin the assessment by choosing their answers from a list of multiple choices provided as seen in figure 5.4.

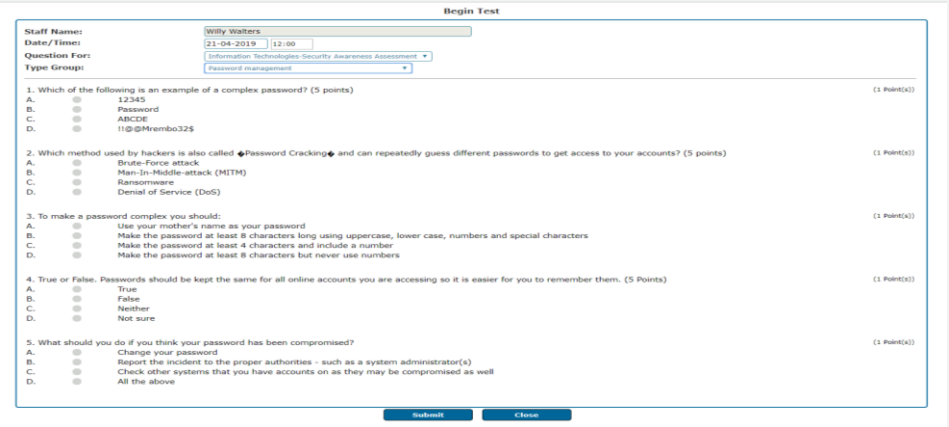



***Figure 5.4: Test Questions***

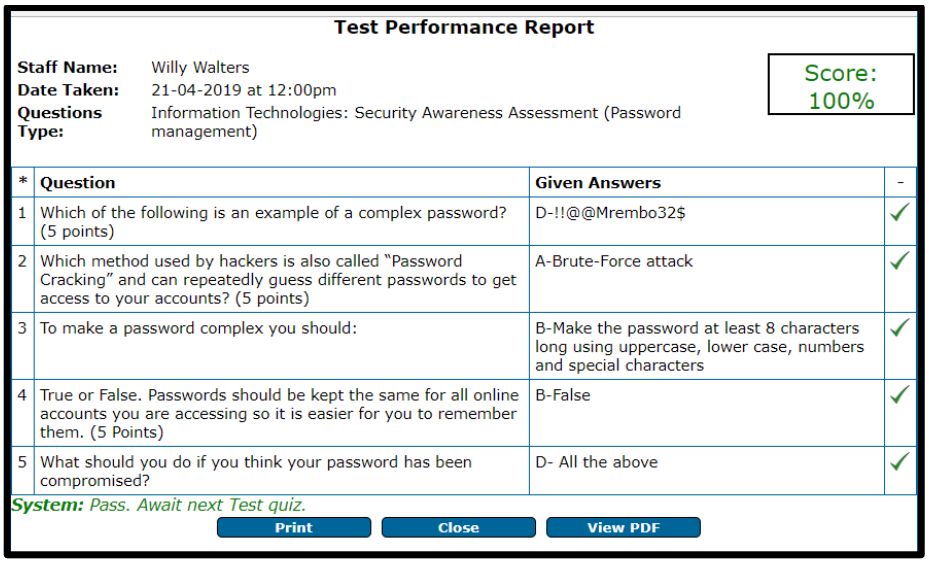



***Figure 5.5: Test Performance Report***

Once the user completes the assessment and submits the questions for marking, the system generates a report of the user's performance along with guidelines on the next step to be taken as shown in figure 5.5. At this point, the second rule for the second decision component found in chapter 2 of the study is applied at this point. If a user passes the assessment test, the decision made by the system is that the employee can now proceed to sit for the next assessment test. However, if the employee fails the assessment test, the decision taken by the system is to recommend that the employee retakes the assessment test.

## 5.6 Testing

The system was subjected to a series of user acceptance tests to ensure that all the functional requirements had been achieved and all the modules work as expected. Various tests were carried out at this stage including unit testing, acceptance testing, system testing and integration testing. The team carrying the testing exercise consisted of individuals from both the technical teams as well as users from different departments. For the technical team there were five software engineers, four software testers and the overall project team leader. They carried tests for a period of four weeks to determine if the system has met the technical specifications and the results of their test were captured in a questionnaire form. The sample form captured in Appendix A of this study.

For the user acceptance testing team, each department provided three users to participate in the exercise and they were drawn from finance, business development, operations, information technology, human resources, operations and legal departments. The users tested the system for a period of two weeks before giving their feedback via a user acceptance test questionnaire. A sample of the questionnaire is captured by the Appendix B section of this study.

### *5.6.1 Unit Testing*

The project team performed tests on each block of code during the development process to ensure that it works properly before being integrated.

### *5.6.2 Integration testing*

This test was carried out on each module before, during and after integration into the overall system to ensure to determine the effect on the entire system.

### *5.6.3 System Testing*

The overall system was tested thoroughly before being released into the live environment. This was achieved by subjecting it to series of stress tests where multiple users from the project team were asked to log in to the system to determine if it could handle the heavy load.

### *5.6.4 User Acceptance Testing*

The complete system was made available for testing to the users in order to determine its ease of use and effectiveness. The users were able to access how long the system takes to respond to their requests, how the test questions are generated and the ease of navigating from one page to the other within the system. The administrators of the system were able to test the system to determine if they can create user profiles and upload test questions without much trouble.

## 5.7 Test Results

After carrying out all the required tests, the following was determined after being captured in the user acceptance test and technical testing questionnaire forms by the respective parties that carried out the tests:

During the integration testing, the bugs discovered by the testing teams within the code for different modules were either repaired or fixed and the system worked well without a hitch as shown in figure 5.5.

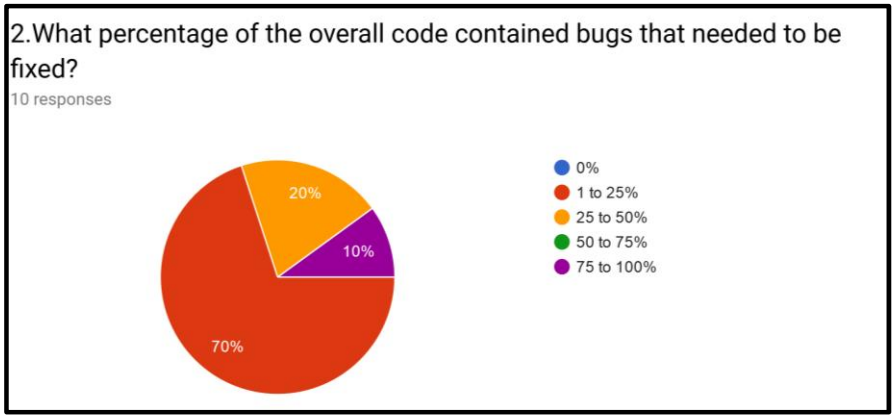



***Figure 5.5: Bugs Detected***

The stress tests revealed that the system is stable enough to handle the load when multiple users log in and use it concurrently. It can handle more than 80 users concurrently without having its performance degraded as depicted by figure 5.6.

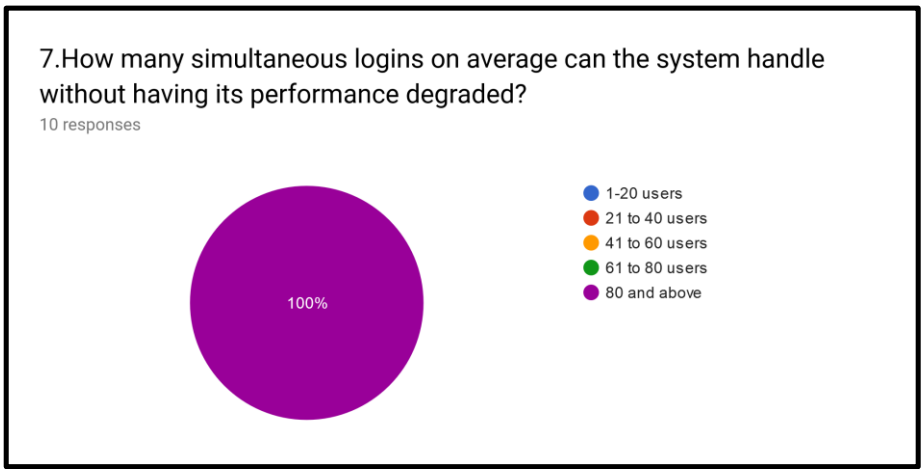



***Figure 5.6: System Robustness***

The user acceptance tests revealed that the system responds well and in a timely fashion to user requests including the generation of the assessment tests and generation of the test report. The overall response time for the system is quite impressive and there is not much variation in the timings when one user is using the system and when there are multiple requests to the system as shown in figures 5.7 and 5.8.

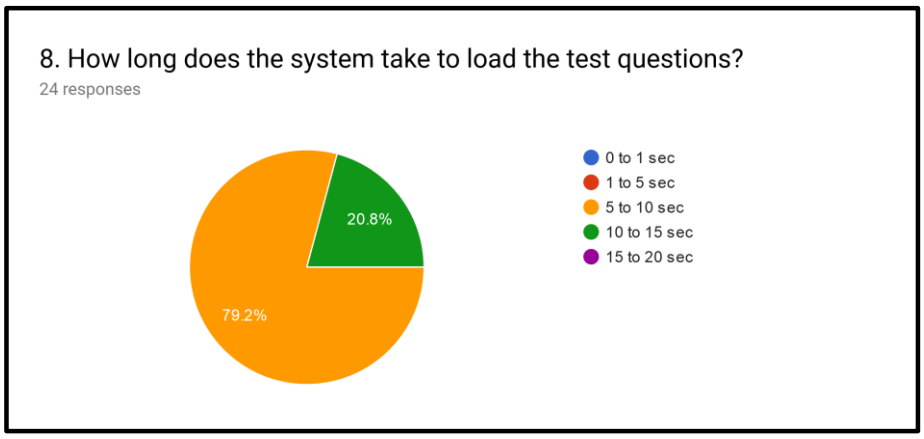



***Figure 5.7: System Response Time When Loading Questions***

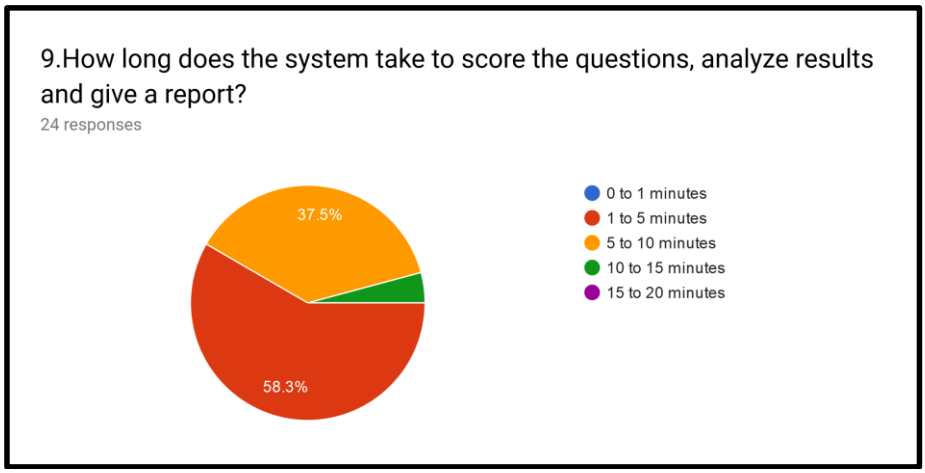



***Figure 5.8: System Response Time When Scoring Questions***

The results also revealed that the system can accurately score and analyse the questions the tests submitted by a user with 100% accuracy rate as seen in figure 5.9.

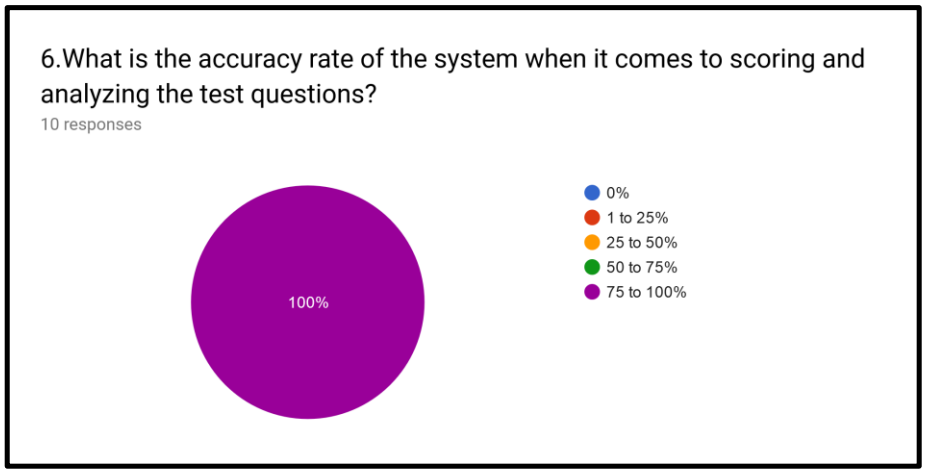



***Figure 5.9: Test Scoring Accuracy***

Input validation tests revealed that the system can capture invalid characters that are keyed in while a user is logging in and gives an error when an invalid entry is made. The system also locks out a user after three unsuccessful logon attempts.

With respect to the user friendliness and ease of use, the user acceptance tests revealed that the system is not complex, and users are able to interact with without requiring any technical assistance as seen in Figures 5.10 and 5.11 below.

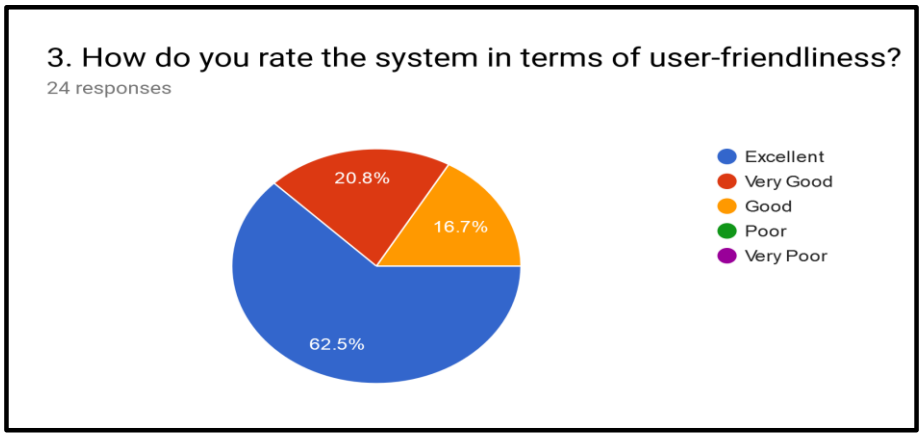



***Figure 5.10: User-Friendliness***

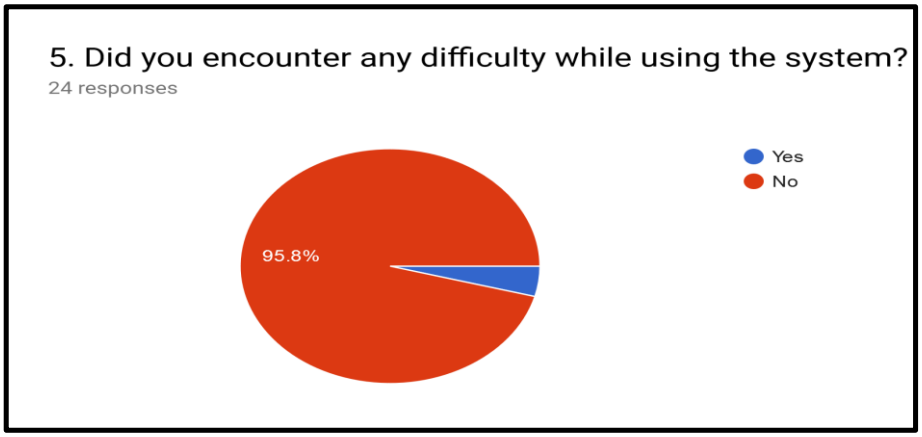



***Figure 5.11: Ease of Use***

In conclusion, all the issues that were discovered by the above tests were resolved and the system was declared ready to be launched into the live environment for use by the employees.

### 5.8 Implementation

The project team carried out training of the system for all employees according to their departments. The appropriate user guides and manuals were developed and distributed to all employees and they were taken through all the relevant functions of the system. Upon completion of the training phase, all employees signed the training sheet confirming that they had had been trained and that they were satisfied with the overall functionality of the system. The system was then launched into the live environment for continuous use.

## Chapter 6: Discussion

The results from this study have been able to comprehensively meet all the objectives outlined in chapter one which were to identify common forms of social engineering attacks that target employees in the financial sector, to review the existing solutions for addressing social engineering attacks, design, develop and test a web-based automated solution for addressing social engineering attacks targeting employees in the financial sector and to validate the effectiveness of the tool or system.

To achieve the first objective, chapter two of this study was able to determine that there are several forms of social engineering attacks that target the financial sector which include dumpster diving, shoulder surfing, google hacking, email spoofing and phishing. Other threats identified were data breaches, abuse of privilege access, malware and insider threats. With respect to insider threats, it was interesting to note that some of them happen due to negligence that results in careless mistakes which can be exploited by attackers.

The second objective was also achieved in chapter two by examining current solutions for countering social engineering attacks through a review of the frameworks proposed by different authors. The first framework by Mathew Spinnapolice suggests that organisations must breakdown their security approach into three categories. These are physical security, digital security and user awareness training. The physical security angle suggests the implementation of physical measures such as access control systems within an office premises to counter piggybacking attempts, auto-locking doors to keep out unauthorised personnel and alarm systems integrated with motion detectors to deter any plans to breach the physical security barriers. Proper disposal of sensitive documents would go a long way towards reducing the risk of dumpster diving attacks. Employees are also discouraged from using their corporate laptops or mobile devices in open public spaces to prevent shoulder surfing attacks. With respect to digital security, organisations are urged to implement multi-factor authentication for all their employees as well as use of virtual private networks as secure communication channels. Email filtering solutions are also suggested as a suitable of countering email phishing attacks. Finally, all organisations are encouraged to carry out some form of user awareness training by taking advantage of various products like phishing simulation tools to subject employees to mock phishing tests. The disadvantage with Mathew Spinnapolice's approach towards countering social engineering attacks is that it does not provide for an all-inclusive approach of testing users preparedness and responsiveness to social engineering attacks. Instead this approach

focuses more on the controls and measures that the organisation can implement to protect itself. It does not empower the employee appropriately to equip him/her with the necessary knowledge that can enable them to respond to a social engineering attack. Additionally, the suggested simulated phishing attacks can be detrimental because they can disrupt the normal flow of work within the office since an employee is likely to get distracted by them. Secondly, panicked employees may cause a lot of disturbance when they flood the IT help desk with distress calls.

The second framework for countering social engineering attacks that this study considered was the adoption of information security from two dimensions. These dimensions are with respect to the function of the control and controls according to the level within the organisation as proposed by Bernard Osterloo. This framework proposes the adoption of preventive, reductive, detective, repressive and corrective controls. In addition to this, the controls at different levels within the organisation should be identified as strategic, operation and tactical controls. The disadvantage with Osterloo's proposed solution is that it does not address the human factor of employee awareness. It focuses more on implementation of security controls without defining any solution on empowering the employee to respond to and counter social engineering attacks.The final framework for mitigating social engineering attacks to be considered by this study was the Social Engineering Defence Framework (SEDF) by Bill Gardner and Valarie Thomas. This framework is split into four phases which include determination of exposure, evaluation of defences, education of workforce and streamlining technology and policy. The limitation with the Social Engineering Defence Framework (SEDF) is that it does not propose any practical way of evaluating an employee's knowledge and preparedness as well as ability to respond to social engineering attacks. Though it has an element of educating the workforce, it does not provide a clearly defined strategy for that other than proposing the execution of simulated attacks. In addition to the above, chapter 2 of this study also explored various existing automated tools for countering social engineering attacks with the aim of determining how they work, their benefits as well their limitations. The tools that were considered include KnowB4, PhishMe, Phish Threat and Phish Insight. Despite the various benefits that these tools provide, this study concluded that these tools are limited by the fact that they solely focus on countering online attack by exposing employees to simulated phishing attacks and they are have no ability to offer any counter measures to the physical forms of social engineering attacks like dumpster diving and shoulder surfing and therefore resulted in the development of a

conceptual framework that would address all the above limitations of the other tools through the development of a web-based knowledge assessment tool known as Cyber Prep.

In order to address the limitations of the existing automated tools for countering social engineering attacks and to meet the third objective, chapters three, four and five of this study led to the design, development and testing of a web-based knowledge assessment tool that can be used to help organisations within the financial services sector to counter social engineering attacks by administering comprehensive assessment tests to employees to gauge their levels of preparedness and their ability to react or respond appropriately to social engineering attacks. The tool was developed using the rapid application development methodology (RAD), which consists of the requirements analysis and gathering stage, the user design stage, the development stage and the product launch or implementation stage.

To achieve the fourth and final objective as demonstrated in chapter five, the system or tool was subjected to various tests to prove that it effectively empowers employees with the ability and skill to respond and react to social engineering attacks. The tests that were conducted include unit tests to confirm that the individual code for each module functions as expected before integration, integration tests to determine how well all the modules work when integrated, system testing to determine the assess the overall functionality against the specified requirements and user acceptance testing for the users to give their approval and overall satisfaction of the system. The results of from the tests were duly captured using test questionnaires for the teams carried out in the tests. A sample of the questionnaires used can be found in the appendix A and appendix B section of this study. Upon completion of all tests the system was officially commissioned to for use by organisations in the financial services sector.

# Chapter 7: Conclusion and Recommendations

## 7.1 Conclusion

The purpose of this research was to develop a web-based assessment tool that can be used by organisations in the financial sector to test and assess how well prepared their employees are in identifying and responding to various forms of social engineering attacks. The tool was developed by implementing all the specifications provided by the project owners and key stakeholders. It was able to address all address all the gaps identified in this research as well as the shortcomings of other mitigation measures identified in chapter 2 of this study. The specific objectives of the study were to identify common forms of social engineering attacks that target employees within the financial sector, to review the existing solutions for mitigating against forms of social engineering attacks, to design, develop and test a web-based automated assessment tool for mitigating against various forms of social engineering attacks in the financial sector and to validate the effectiveness of the automated tool. The first and second objectives were achieved in chapter 2 by a review of existing literature and documentation to assist in identifying forms of social engineering attacks and establishing any existing tools for mitigating against social engineering threats. The existing solutions identified were further analysed to expose their benefits and shortcomings. The third and fourth objectives were achieved through the design development, testing and implementation of the cyber prep web - based assessment tool. The validation of the tool was carried out through user acceptance tests and attestation from the key stakeholders of the project that it had met its intended objective.

## 7.2 Recommendations

The tool works remarkably and can analyse employee's preparedness to respond and react to social engineering by assessing them through a series of pre-defined questions that result in the employee being scored and graded. The report produced by the system enables the organisation to determine their employee's level of vulnerability based on their performance in the test. This study proposes that further improvements be made to the tool to ensure that it is incorporated into performance appraisal process for all organisations in the financial service sector. This would make sure the employees take these tests more seriously when it is tied to their appraisal as the human resource office can embed it within the performance review system.

## 7.2 Future Work

This the study was confined to addressing social engineering attacks in the financial sector, but this can also be extended towards looking into social engineering attacks in other sectors. The

study also recommends that the scope be extended to look into not just social engineering attacks but also other types of attacks.

## References


Accenture. (2017). *Cost of Cyber Crime Study.* Retrieved from www.accenture.com: https://www.accenture.com/.../PDF.../Accenture-2017-CostCyberCrimeStudy.pdf

Acunetix. (2019). *Google Hacking*. Retrieved 2019, from Acunetix: https://www.acunetix.com/websitesecurity/google-hacking/

Airehrour, D. (2018). *David Airehrour.* Retrieved from MDPI: https://www.mdpi.com/2078-2489/9/5/110/htm

Alhaji Idi Babate, M. A. (2014). State of Cyber Security: Emerging Threats Landscape. *International Journal of Advanced Research in Computer Science & Technology, Vol. 3*(Issue 1 (Jan. - Mar. 2015)), 1. Retrieved 2019, from https://www.ijarcst.com/doc/vol3issue1/ver2/alhaji.pdf

Avanessian, A. (2017, April 21). Retrieved from Bobsguide.com: https://www.bobsguide.com/guide/news/2017/Apr/21/why-social-engineering-remains-a-threat-to-fintechs/

Campanelli, A. (2018). *Lessons Learned from 3 Major Financial Services Data Breaches*. Retrieved 2019, from www.bitsight.com/: https://www.bitsight.com/blog/lessons-learned-from-3-major-financial-services-data-breaches

Castle, S. (2007). *News.* Retrieved 2019, from Independent.co.ke: https://www.independent.co.uk/news/world/europe/thief-woos-bank-staff-with-chocolates-then-steals-diamonds-worth-16314m-5332414.html

Chizari, H. (2015). Social Engineering Attack Mitigation. *International Journal of Mathematics and Computational Science, 1*(4). Retrieved 2018, from https://www.researchgate.net/publication/307606034_Social_Engineering_Attack_Mitigation

Confense. (2019). Retrieved from Confense: https://cofense.com/product-services/phishme/

Cyberarms. (2010). *Social Engineering: Tips to Defend against Shoulder Surfing*. Retrieved 2019, from Cyberarms: https://cyberarms.wordpress.com/2010/05/01/social-engineering-tips-to-defend-against-shoulder-surfing/

CyberSheath. (2014). *Cybersheath Privileged Breaches.* Retrieved 2018, from Cybersheath.com: https://www.cybersheath.com/wp-content/.../CyberSheath_Privileged_Breaches.pdf

Gregg, M. (2006). *Hack in The Stack.* (S. Watkins, Ed.) Rockland, Massachusetts, U.S.A: Syngress Publishing, Inc. Retrieved 2019, from https://doc.lagout.org/security/Syngress.Hack.the.Stack.Oct.2006.pdf

Hammoudeh, J. S. (2018). Defense Methods Against Social Engineering Attacks. Retrieved 2019, from https://www.researchgate.net/publication/319097404_Defense_Methods_Against_Social_Engineering_Attacks

Henley, M. (2019). *Phishing Attacks in the Financial Industry*. Retrieved 2019, from resources.infosecinstitute.com: https://resources.infosecinstitute.com/category/enterprise/phishing/the-phishing-landscape/phishing-attacks-by-demographic/phishing-attacks-financial-industry/#gref

Hooper, B. (2018). *Secure Email Gateway*. Retrieved 2019, from Astrix: https://astrix.co.uk/news/2018/11/26/how-to-mitigate-email-spoofing/#SecureEmailGateway

IBM. (2018). *Global Cost of A Data Breach.* Retrieved 2019, from databreachcalculator.mybluemix.net: https://databreachcalculator.mybluemix.net/.../2018_Global_Cost_of_a_Data_Breach_...

KnowB4. (2019). *About us*. Retrieved from KnowB4: https://www.knowbe4.com/about-us/

Korkishko, I. (2017). Top 6 software development methodologies. Retrieved 2019, from Top 6 software development methodologies

Lockheed Martin Corporation. (2015). *Financial Services Cyber Threats.* Retrieved 2019, from CIO Summits: https://www.ciosummits.com/Financial_Services_Cyber_Challenges_White_Paper.pdf

Morgan, S. (2017). *2017 Cybercrime Report.* Retrieved 2018, from https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

Office of the Australian Information Commissioner(OAIC). (2018). *Data breach preparation and response.* Retrieved 2018, from OAIC: https://www.oaic.gov.au/resources/...and.../data-breach-preparation-and-response.pdf

Oosterloo, B. (2008). Retrieved February 22, 2019, from Essay.Utwente: https://essay.utwente.nl/59233/1/scriptie_B_Oosterloo.pdf

Ornaghi, A. (2003). Retrieved 2019, from Blackhat.com: https://www.blackhat.com/presentations/bh-europe-03/bh-europe-03-valleri.pdf

Osterloo, B. (2008). Retrieved 2019, from essay.utwente.nl: https://essay.utwente.nl/59233/1/scriptie_B_Oosterloo.pdf

Pandove, K. (2010). Retrieved 2019, from Citeseerx: citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.206.5745&rep=rep1...pdf

Pascu, L. (2018). *White papers.* Retrieved 2019, from Bitdefender.com: https://www.bitdefender.com/business/whitepapers.html

Petters, J. (2018). *Insider Threats*. Retrieved 2019, from Varonis: https://www.varonis.com/blog/insider-threats/

Purdy, A. (2016). *Media Kit.* Retrieved 2019, from Huawei: https://www-file.huawei.com/-/media/CORPORATE/PDF/cyber-security/the-global-cyber-security-challenge-en.pdf

Raytheon. (2014). *Capabilities.* Retrieved 2018, from Raytheon.com: https://www.raytheon.com/capabilities/rtnwcm/groups/cyber/.../rtn_257010.pdf

Rouse, M. (2005). *Shoulder surfing*. Retrieved 2019, from Techtarget: https://searchsecurity.techtarget.com/definition/shoulder-surfing

Sachkov, I. (2017). *polygon*. Retrieved 2019, from Group IB: https://www.group-ib.com/blog/polygon

Saleem, J. S. (2012). Retrieved 2019, from https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2014/...final/report.pdf

Schaffer, P. (2018, March 26). Retrieved from cpomagazine.com: https://www.cpomagazine.com/cyber-security/impact-cybersecurity-incidents-financial-institutions/

Sentinel One. (2016). *Ransomware.* Retrieved 2019, from Sentinel One: https://go.sentinelone.com/rs/327-MNM-087/.../SentinelOne_Ransomware_0116.pdf

SentinelOne. (2016, August). *The Most Devastating Cyber Attacks on Banks*. Retrieved 2019, from sentinelone.com: https://www.sentinelone.com/blog/the-most-devastating-cyber-attacks-on-banks/

Serianu. (2017). Retrieved from Serianu.com: https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf

Serianu Limited. (2018). *Serianu Cyber Security Report 2018.* Nairobi: Serianu Limited. Retrieved 2019, from https://www.serianu.com/resources.html

Sharp, R. (2007). *An introduction to Malware.* Retrieved 2019, from DTU Orbit: http://orbit.dtu.dk/en/publications/an-introduction-to-malware(edb48936-1d23-472a-897b-187a0f0c4a7c).html

Social Engineer. (2018). Retrieved 2018, from Social Engineer: https://www.social-engineer.com/vigilant-dumpster-diving-attack/

Solid state systems. (2019). *prevent man-in-the-middle-attacks*. Retrieved 2019, from Solid system state: http://solidsystemsllc.com/prevent-man-in-the-middle-attacks/

Sophos. (2019). Retrieved from Sophos: https://www.sophos.com/en-us/products/phish-threat.aspx

Spinapolice, M. (2011). Mitigating the risk of social engineering attacks. Retrieved 2019, from scholarworks.rit: scholarworks.rit.edu/cgi/viewcontent.cgi?article=1397&context=theses

Stoy, D. (2018). Retrieved 2019, from Cordinated Blog: https://www.coordinated.com/blog/why-mock-phishing-might-catch-you-more-grief-than-good-with-your-employees

The App Solutions. (2018). *Rad Model*. Retrieved 2019, from The App solutions: https://theappsolutions.com/blog/development/rad-model/

The Ponemon Institute. (2017). *2017 Cost of Cyber Crime Study.* The Ponemon Institute. Retrieved 2018, from https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

Thomas, B. G. (2014). *Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats.* Wlatham, Massachussets, U.S.A: Syngress. Retrieved 2019, from https://www.researchgate.net/publication/291092430_Building_an_Information_Security_Awareness_Program_Defending_Against_Social_Engineering_and_Technical_Threats_1st_Edition

Trend Micro. (2019). Retrieved from Trend Micro: https://phishinsight.trendmicro.com/en/

Vasco. (2015). *Social Engineering.* Retrieved 2019, from Vasco.com: https://www.vasco.com/images/Social-engineering_tcm42-46728.pdf

Wainainah, D. (2019). *Corporate*. Retrieved 2019, from www.businessdailyafrica.com: https://www.businessdailyafrica.com/corporate/tech/4258474-5055282-89ehu1z/index.html

Weippl, E. (2014). Advanced social engineering attacks. *Journal of Information Security and Applications*. Retrieved 2019

Zhang, E. (2018). *The Top 10 FinServ Data Breaches*. Retrieved 2019, from digitalguardian.com: https://digitalguardian.com/blog/top-10-finserv-data-breaches

## Appendix A: Technical Testing Questionnaire

**Name of Tester:** **Department:**

**Title:** **Date:**

1. **Do all the system modules integrate well with each other?**

   Yes☐ No☐

2. **What percentage of the overall code contained bugs that needed to be fixed?**

   0% ☐ 1% to 25%☐ 25% to 50%☐ 50% to 75% ☐ 75% to 100% ☐

3. **What is the overall response rate of the system when only one user has logged in to take the test?**

   0-1 minute☐ 1-5 minutes☐ 5-10 minutes☐ 10-15 minutes ☐ 15-20 minutes ☐

4. **What is the overall response rate of the system when multiple users have logged in to take the test?**

   0-1 minute☐ 1-5 minutes☐ 5-10 minutes☐ 10-15 minutes ☐ 15-20 minutes ☐

5. **How many simultaneous logins on average can the system handle without having its performance degraded?**

   1-20 users☐ 21-40 users☐ 41-60 users☐ 61-80 users☐ 81 to 100users☐

6. **What is the overall response rate for typing, cursor and mouse movements?**

   0-1 sec☐ 1-5 sec☐ 5-10 sec☐ 10-15 sec ☐ 15-20 sec ☐

7. **What is the accuracy rate of the system when it comes to scoring and analysing the test questions?**

   0% ☐ 1% to 25%☐ 25% to 50%☐ 50% to 75% ☐ 75% to 100% ☐

## Appendix B: User Acceptance Testing Questionnaire

**User Name:** **Department:**

**Title:** **Date:**

1. **How do you rate the functionality of the system?**

   Excellent☐ Very Good☐ Very Good☐ Poor☐ Very Poor☐

2. **How do you rate the graphical user interface design of this system?**

   Excellent☐ Very Good☐ Very Good☐ Poor☐ Very Poor☐

3. **How do you rate the system in terms of user-friendliness?**

   Excellent☐ Very Good☐ Very Good☐ Poor☐ Very Poor☐

4. **How do you rate the operational performance of this system?**

   Excellent☐ Very Good☐ Very Good☐ Poor☐ Very Poor☐

5. **Did you encounter any difficulty while using the system?**

   Yes☐ No☐

6. **Did you feel secure and comfortable and secure using the system?**

   Yes☐ No☐

7. **How long does the system take to authenticate you while logging in?**

   0-1 minute☐ 1-5 minutes☐ 5-10 minutes☐ 10-15 minutes ☐ 15-20 minutes ☐

8. **How long does the system take to load the test questions?**

   0-1 minute☐ 1-5 minutes☐ 5-10 minutes☐ 10-15 minutes ☐ 15-20 minutes ☐

9. **How long does the system take to score the questions, analyse results and give?**

   0-1 minute☐ 1-5 minutes☐ 5-10 minutes☐ 10-15 minutes ☐ 15-20 minutes ☐

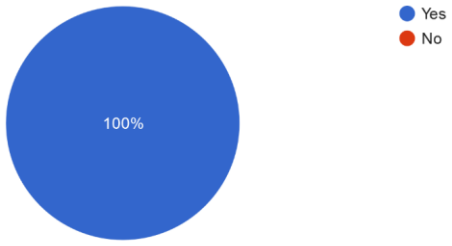
10. **Is the system able to accurately score the test questions?**

    Yes☐ No☐

## Appendix C: Technical Test Findings

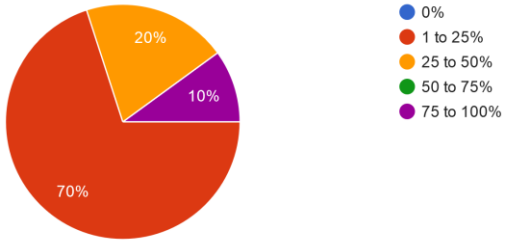
1.Do all the system modules integrate well with each other?

10 responses



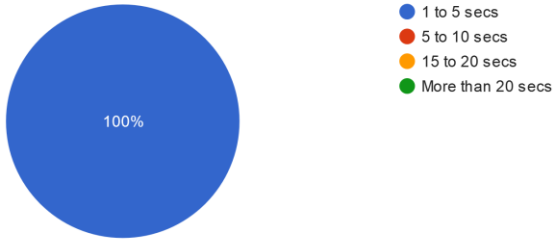

2.What percentage of the overall code contained bugs that needed to be fixed?

10 responses



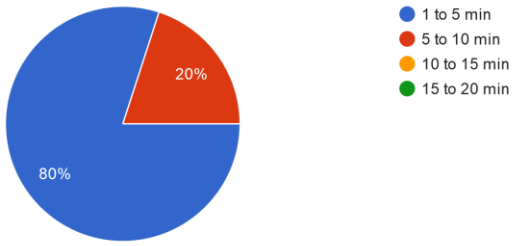

3.What is the overall response rate of the system when only one user has logged in to take the test ?

10 responses



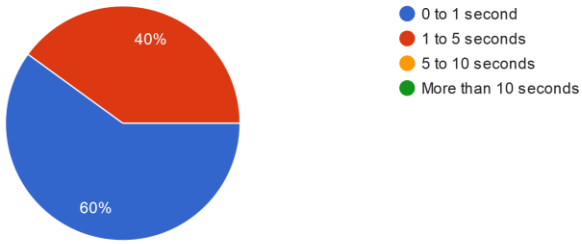
4.What is the overall response rate of the system when multiple users have logged in to take the test ?

10 responses



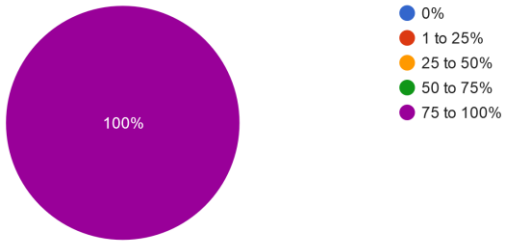

5.What is the overall response rate for typing, cursor and mouse motions or movements

10 responses




6.What is the accuracy rate of the system when it comes to scoring and analyzing the test questions?

10 responses



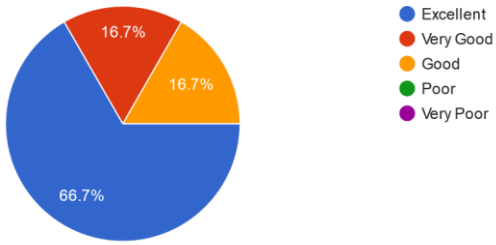
7.How many simultaneous logins on average can the system handle without having its performance degraded?

10 responses

## Appendix D: User Acceptance Test Results

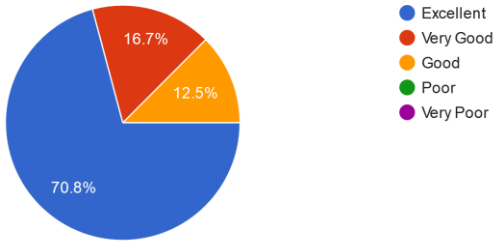
1.How do you rate the functionality of the system?

24 responses



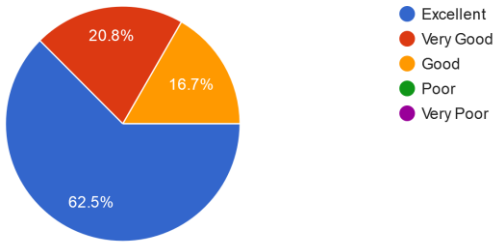

2.How do you rate the graphical user interface design of this system?

24 responses



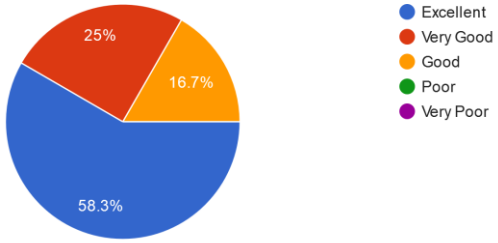

3. How do you rate the system in terms of user-friendliness?

24 responses



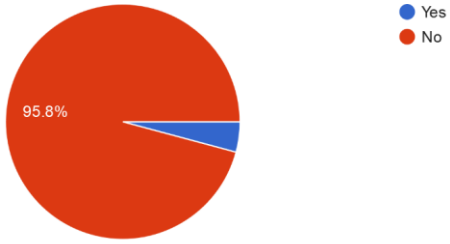
4. How do you rate the operational performance of this system?

24 responses



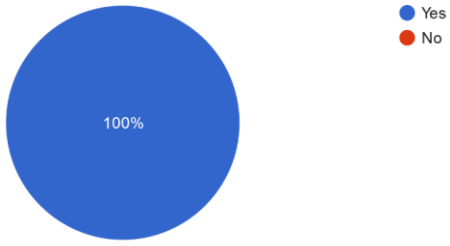

5. Did you encounter any difficulty while using the system?

24 responses



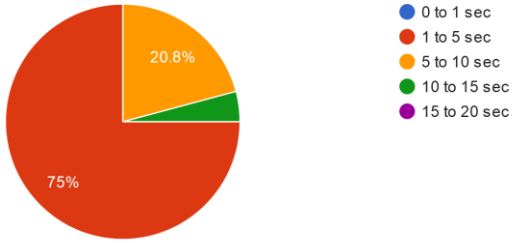

6.Did you feel secure and comfortable using the system?

24 responses



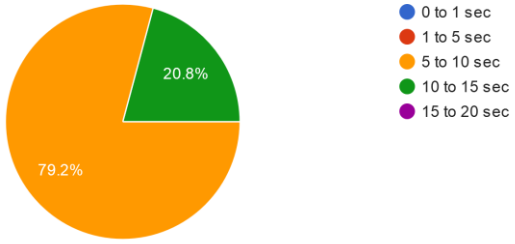
7.How long does the system take to authenticate you while logging in?

24 responses



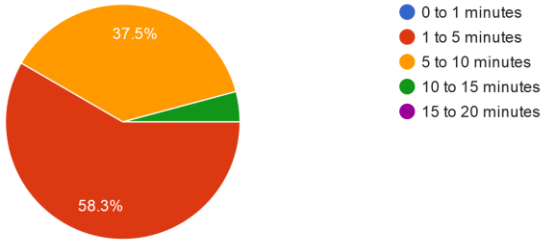

8. How long does the system take to load the test questions?

24 responses



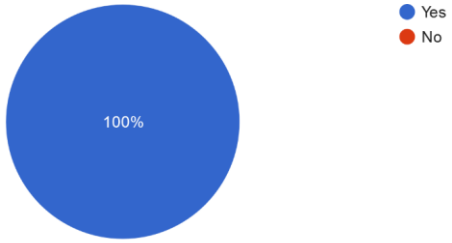

9.How long does the system take to score the questions, analyze results and give a report?

24 responses



10. Is the system able to accurately score the test questions?

24 responses



# Appendix E: Cyber Prep App Test Questions

## Email Security Questions

1. An email that attempts to trick a reader into installing software that may contain a virus or ask for confidential information is an example of a: (1 Point(s))

A. Phishing scam
B. Brute-Force attack
C. Fishing scam
D. Dumpster diving attack

2. What is the best definition of Spear Phishing? (1 Point(s))

A. A random email sent to a massive group of users
B. A malicious virus that can encrypt or lock your computer
C. A phishing email aimed directly at you
D. A method hackers use to guess your password

3. If you get a suspicious phone call at work from a representative at Microsoft claiming that your computer is infected with a virus, you should: (1 Point(s))

A. Hang up and contact your supervisor immediately
B. Provide them with your login credentials
C. Allow them to login remotely to your computer so they can assist you
D. Allow them to help you install or remove a program

4. A customer service representative has just called you saying that your credit card is about to expire, he or she asked you to provide your account information and personal information in order to verify your account and to renew your credit card without telling you from what bank he or she came from. What should you do? (1 Point(s))

A. Ask the customer representative what bank or company he or she is from.
B. Verify your credit card if it really expired because expiration dates are placed on credit cards
C. Verify your credit card if it really expired because expiration dates are placed on credit cards
D. All of the above

5. When receiving an email from an unknown contact that has an attachment, you should: (1 Point(s))

A. Open the attachment to view its contents
B. Delete the email
C. Forward the email to your co-workers to allow them to open the attachment first
D. Forward the email to your personal email account so you can open it at home

## Insider Threats

1. When a busy office manager allows a visitor to navigate through your office without an escort, what do you call this type of a threat? (5 Points) (1 Point(s))

A. Malware
B. Phishing
C. Denial of Service (DoS)
D. Insider threat

2. Which of the following life experiences might turn a trusted user into a malicious insider except: (1 Point(s))

A. Frustration with co-workers
B. Stress
C. Promotion
D. Financial problems

3. The following are all behavioral signs or indicators of an insider threat except one. Which could it be? (1 Point(s))

A. Downloading large amounts of data
B. Frequently in the office during off hours
C. Arriving to work on time
D. Display of disgruntle behavior towards co-workers

## Physical Security

1. How can you protect sensitive data from office visitors? (1 Point(s))

A. Keep your office doors open all day
B. Allow them walk around the office without an authorised escort
C. Give them your password but only for your computer
D. ● Track all office visitors and restrict their access to certain areas within the office.

2. All of these are good physical security practices except? (1 Point(s))

A. ● Always wear your security badge when leaving work, even if just for a break. They should be worn outside of the office in public so other people know where you work
B. Control access to your office by ensuring the door closes completely behind when entering and exiting. Ensure that no one slips in behind you
C. When working in a public setting, prevent shoulder surfing by shielding your paperwork and keyboard from view using your body
D. Follow the Clear Desk and Screen Policy. Store confidential and sensitive items in a secure place

3. You see a non familiar face in the access controlled areas of our office, the person does not have an ID/Visitor/Staff/Vendor tag with him. What would you do? (1 Point(s))

A. None of my business, let some body else take care of it
B. Ask the person to leave the facility
C. ● Escort the person to the security and raise a security incident
D. Raise a security incident and go back doing your work

4. It's almost lunch and you are not done working on your report. Which the following should be the first thing for you to do before you leave your desk? (1 Point(s))

A. Inform your supervisor that you are going out for lunch
B. Ask your colleague to accompany you
C. Check for your wallet befor eleaving the office
D. ● Lock your computer

## Proper Password Management

1. Which of the following is an example of a complex password? (5 points) (1 Point(s))

A. 12345
B. Password
C. ABCDE
D. ● !!@@Mrembo32$

2. Which method used by hackers is also called ﷺPassword Crackingﷺ and can repeatedly guess different passwords to get access to your accounts? (5 points) (1 Point(s))

A. ● Brute-Force attack
B. Man-In-Middle-attack (MITM)
C. Ransomware
D. Denial of Service (DoS)

3. To make a password complex you should: (1 Point(s))

A. Use your mother's name as your password
B. ● Make the password at least 8 characters long using uppercase, lower case, numbers and special characters
C. Make the password at least 4 characters and include a number
D. Make the password at least 8 characters but never use numbers

4. True or False. Passwords should be kept the same for all online accounts you are accessing so it is easier for you to remember them. (5 Points) (1 Point(s))

A. True
B. ● False
C. Neither
D. Not sure

## Appendix E: Turnitin Report