INFORMATION SYSTEM SECURITY THREATS AND VULNERABILITIES: EVALUATING THE HUMAN FACTOR IN DATA PROTECTION

By

Omar Safianu (20091978) (PG6559311)

A thesis submitted to the Department of Computer Science, Kwame Nkrumah University of Science and Technology in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

April 2016

DECLARATION

I wish to state that this work came from my own efforts towards the MSc and I pledge that all thoughts and ideas in the thesis are mine and are not the thoughts or materials previously published by another person. Any ideas, thoughts or materials used in this study have been duly acknowledged.

Omar Safianu (20091978; PG6559311)	……	……
Student Name and ID	Signature	Date

Certify by:

Dr. J. B. Hayfron-Acquah	……	……..
(Supervisor)	Signature	Date

Certify by:

Dr. J. B. Hayfron-Acquah	……	……..
(Head of Department)	Signature	Date

DEDICATION

This thesis is dedicated to my Dad and Mum, and to my Son and Wife.

AKNOWLEDGEMENTS

Finishing this thesis would not have been possible without the assistance and support of friends and family around me which is only possible to mention some of them here.

First, I want to acknowledge my enormous gratitude to God who gave the protection and energy.

There are no proper words to convey my deep appreciation for my thesis supervisor, Dr. J. B. Hayfron-Acquah, who, despite his many academic commitments, agreed to supervise my work. His criticism and comments on my work inspired and motivated me.

All the respondents (I am cautious of mentioning where I took my samples for security reasons) who participated in this research project with interest and enthusiasm.

Last but not least, I would like to express my gratitude to my family, especially my parents, my wife and son for supporting me spiritually throughout the research period.

ABSTRACT

Researches in information security have all these while been concerned only with technical problems. Attempts to curb security problems are either software-centered or hardware-oriented. The greatest loophole in information security are people who use the computers. However, there have been limited attempts in addressing the people aspect of security.

In this study the missing link in information security, that is, the end-user working on the system is addressed. Despite the implementation of technological solutions, the human factor is still vulnerable to attacks and hence in need of further investigation and interrogation.

The study draws its data from a survey conducted on people who frequently use information systems. Professional and technical inputs were also solicited from IT personnel through interviews. Four experiments were conducted to test the accuracy of the survey. A phony phish system was developed to test respondents' information security. The goal of the phony phish system is to send phishing emails that can be used to measure the accuracy of the survey. The rest of the experiments were SQL injection, cross site scripting and brute force attack.

The thesis argues that advancement in security technologies do not always guarantee secure environments. Thus, information security cannot be depended exclusively on hardware or software. It is people who use computers and therefore information security is also a human factor

issue. It also suggests, for information and data breaches to be curbed, organizations must adopt a holistic security framework, incorporating the human factor vulnerability to it.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

IDS	Intrusion Detection System
VA	Vulnerability Assessment
FTP	File Transfer Protocol
DNS	Domain Name System
DES	Data Encryption Standards
AES	Advanced Encryption Standards
DoS	Denial of Servive
IPS	Intrusion Prevention System
IT	Information Technology
XSS	Cross Site Scripting

CHAPTER ONE

INTRODUCTION

1.1 Background

Information security refers to the protection of the confidentiality, integrity and access to information (Kruger and Kearney, 2006). Institutions face security problems despite allocating a big budget for technical controls (Besnard and Arief, 2004). In the 2007 CSI Computer Crime and Security Survey it was concluded that although 98% of users have anti-virus software, 52% were still infected with viruses (Richardson, 2007). This suggests that information security is not only a technological problem, but is also a 'people' problem because a technological solution used in the best manner cannot completely protect a system. Chan, Woon and Kankanhalli (2005) advocate that people's ineptitude towards information security guidelines is the cause of major breaks in information security. Again, results of the 2007 Global Security Survey in which information security professionals were surveyed, pointed out that 79% of respondents identify human actions to be the origin of information systems security failures.

Of late, efforts to improve Information Security have been software-centred or hardwareoriented. So far, there have been limited attempts in addressing the people who use the computers. Recent studies have shown that the major loose end to information security are the people who use computer systems. To further highlight that humans are the weakest link in information security, Mitnick and Simon (2002) explain that an organization may have installed the finest security technologies in existence and safeguard their physical structures but it is still totally vulnerable because humans can be the weakest link to the system.

Information security has to integrate "people-ware" to the security framework. Regrettably, quite a number of institutions limit security to hardware and software solutions. In the perspective of

this research, human factors in information security comprise all those activities unintentionally made by end users, that put information at risk in spite of installing all the technological measures such as firewalls, Intrusion Detection Systems (IDS) and anti-virus. In other words, the human factor constitutes all those unintended tasks that can put the security of the system at risk. These tasks include improper use of login credentials, input errors, not logging out of systems, not adhering to security measures, ignorance, and sharing of passwords. The aforementioned actions are opposed to insider threat which is intentional action meant to attack a system by employees entrusted to work with an information system.

This research study therefore addresses the end user working with the information system which has been gloss over by experts in security studies. It is hoped that the vulnerabilities that the study highlighted and the recommendations given will help individuals and organizations to have a second look at their information security infrastructure.

1.2 Problem Statement

Studies in improving information security and the technology associated with it, hitherto, have been concentrated on software or hardware. Many studies have ignored the people who use the computers even though they are the greatest loophole in information systems security. Information systems can be open to attacks even if the finest technological measures such as firewall, Intrusion Detection System (IDS) and antivirus are installed. The reason is that information security is not limited to the technological aspect but incorporates the system users.

Arguably, the greatest loophole to an institution's information security is its own workers because they are the closest threat-agents to the institutional data. It is because it is the workers who use data to conduct the organization's business and therefore their blunders represent a serious threat

to the integrity and security of data as compared to the threats from outsiders. For example, allowing classified information in computers and devices in an unprotected manner is as much a threat to the information as the attacker who seeks to exploit the information. It is therefore important to examine the human factors as potential threat-agents in an Information Technology environment.

Therefore this research addresses the missing link in information security, that is, the end-user working on the system. Technological solutions have improved over the years. However, the human factor is still an issue that needs to be addressed.

1.3 Aims and Objectives

The overall aim of the research is to evaluate the vulnerabilities to information systems by focusing on the human factors. The research seeks to realize the following objectives.

- To highlight the human factors to information security threat;
- To analyze the causes of the human factors which lead to information system security vulnerability;
- To develop a phony phish system that can be used to send phishing emails in order to measure the accuracy of the survey.
- To design a model for the human errors (factors) in information system security.
- To give recommendations in curbing the human factor vulnerabilities.

1.4 Organization of Work

The project is organized in five chapters as follows. Chapter one contains the introduction to the project which include background, statement of the problem, aims and objective, and organization of work. Chapter two discusses Literature review while chapter three presents the research

methodology. Chapter four covers the analysis of results and the last chapter, chapter five, covers the findings, conclusions, and recommendations.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter makes a critical review of existing literature related to the study. Research works and projects from journals, books and electronic resources were cited with the objective of revealing contributions and gaps in studies related to security vulnerabilities.

2.2 Related studies

Several studies have identified areas of vulnerability in information assets of individuals and organizations but none of them touch on the human factor. For instance, Smith (2004) conducted a test to show how data are insecure in organizations. He performed an information security review of publicly accessible servers of the GIAC enterprise. The methodology he used was to examine the public servers from both the network perspective as well as from the local host perspective. The findings of the assessment include:

- Operating systems are not up to date with the latest system updates and security updates.
- The apache server is vulnerable to attacks and is running default configuration
- The Domain Name System (DNS) server has not been locked down.
- The File Transfer Protocol (FTP) server authenticates users using insecure methods.
- The mail server authenticates users in clear-text when encrypted methods are available.

The conclusion was that the information assets of the organization are vulnerable and data and information are insecure.

A similar test was carried by Honeywell's Industrial IT Solutions (2012) in an attempt to help AmerChem company better understand their current cyber security situation, the potential risks associated with that current status, and a proposed path put forward to remediate any issues. The

scope of the audit was all cyber assets at the AmerChem facility. In total, thirty-nine (39) servers and workstations were audited. The findings were that Cyber assets have not been patched since their installation dates; Default Guest accounts is enabled on a number of cyber assets; There are early indications of hard drive failure on one cyber asset; One cyber asset is connected to both the process control network and the business network; and Cyber assets are not up to date, or do not have any malicious software prevention solution in place. Silver (2013), James et al. (2009), Philip et al. (2003) and Anita, Kavita and Kiraandeep (2013) have followed the same trend on concentrating vulnerability evaluation on hardware aspect of information assets but then again the human factor is short of which this research will address.

Studies have been undertaken to identify some of the weaknesses and vulnerabilities in most commonly used cryptographic algorithms. Though studies on cryptosystems vulnerabilities and this research are related one is purely technical and software based and the other focuses on the human aspect of vulnerabilities.

A cryptosystem is an encryption method or process encompassing the algorithm, key(s) or variables(s), and procedures used to perform encryption and decryption (Michael & Herbert, 2005:346). Generally, cryptographic algorithms are mostly grouped into two broad categories-symmetric (also called "private key") encryption and asymmetric (also called "public key") encryption.

Encryption is a valuable tool in securing the confidentiality of information that is in storage and/or transmission. However, weaknesses in the encryption algorithms allow unauthorized access to secure communication. Michael and Herbert (2005:384) posit that today's encryption and cryptosystems are designed in a sophisticated manner but they do exhibit the same flaw that the first systems contain thousands of years ago. If the key (the method used to perform the encryption)

is discovered the message can be determined. They concurred that key management is not so much the management of technology but rather the management of people. They, however, did not show how managing people or how the human factor could address the vulnerabilities in encryption algorithms.

Soomro et al. (2013) stipulate that cryptosystems are even more vulnerable to attacks when they are dealing with small amount of data. The standard symmetric techniques which are usually used for large amount of data such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES) prove to be inefficient for small amount of data encryption due to producing much overhead and increase complexity. They proposed a technique to reduce the inefficiency in the algorithm by introducing XOR operation in the major steps of the symmetric algorithm in order to reduce communication overhead in transmitting small amount of data.

The breaking of every new cryptosystem makes it imperative for researches to shift attention to other methods of protecting data and one of such methods is evaluating the human factor. Security can be compromised in any software or hardware system. The DES system which was initially thought to be secured has been broken into by differential cryptanalysis. Matsui (1994) implemented differential cryptanalysis with C language programs to obtain a linear approximate expression of a given DES cipher algorithm. The findings were that the DES algorithm is vulnerable to attack in that:

- 8-round DES is breakable with 2^{21} known plaintexts in 40 seconds
- 12-round DES is breakable with 2^{33} known plaintexts in 50 hours
- 16-round DES is breakable with 2^{47} known plaintexts in faster than an exhaustive search for 56 key bits

Elbaz and Bar-El (2000) found out that the DES algorithm suffers from *Simple Relations* in its keys. They argue that the complementary relationship between keys results in a complementary relationship between the resulting ciphertexts. This vulnerability reduces the algorithm strength by one bit.

The AES system which is the most advanced method for encryption is not flawless. Cryptography researchers have identified a weakness in the AES security algorithm that can crack secrete keys faster than before (Bogdanov, Khovratovich and Rechberger, 2011). Though the attack has no practical implications on the security of user data, the result is the first theoretical break of the AES security system – the de facto worldwide encryption standard.

The list of encryption algorithms – both symmetric and asymmetric- and their vulnerabilities cannot be exhausted here. Indeed Elbaz and Bar-El (2000) outlined all the known encryption algorithms and their weaknesses. However, their study was based solely on the algorithm (software), ignoring the human factor.

One of the major areas of information security weakness discussed in the literature is on database vulnerabilities. Here again, the vulnerabilities are software and hardware related. The human factor has been glossed over. For instance, Shulman (2006) outlines ten vulnerabilities associated with database infrastructures but none of them talked about the activities end users do that make information systems vulnerable to attacks.

In today's businesses, database technologies are needed more than before and with the increasing usage of the internet for business, threats or risks to these databases are growing. Lamar (2012) opines that database attacks are prevalent these days because of the following vulnerabilities which are summarized below:

- Vulnerabilities in Operating Systems like Windows, UNIX and Linux and their services associated with the databases could create a loophole for illegal access which may lead to a Denial of Service (DoS) attack.
- Database rootkits: A database rootkit is a program or a procedure that is hidden inside the database and that gives the administrator special privileges to be able to access data in the database. Sometimes the rootkits turn off alerts prompted by Intrusion Prevention Systems (IPS) which could be disastrous..
- Weak authentication: Weak authentication models permit attackers to use tactics like social engineering and brute force to get hold of database login details of users.
- Weak audit trails: A weak audit logging method in a database server is risky to an institution particularly in retail, financial, healthcare, and other businesses with strict regulatory observance. PCI, SOX, and HIPAA are rules that require extensive logging of actions and also generate events when something goes wrong. In order to resolve issues when something goes wrong, logging to critical transactions in a database must be done in an automated way. Audit trails work as the last line of database defense and can sense any violation. Audit trails can help trace back the violation to a particular period and a particular user.

Researchers in information security tend to give their attention to only software and hardware as indicated above. This study will add to the literature by looking at a different angle to information systems vulnerabilities, thus, targeting only the end users.

Firewall vulnerabilities have also been discussed in the literature. Firewalls guard a trusted network from an untrusted network by filtering traffic by following a designated security policy.

Different firewalls are being used today and they are one of the sources of security vulnerabilities. Kamara et al. (2010) give a taxonomy to understand firewall vulnerabilities in the framework of firewall implementations as it is not practical to study and test each firewall for all possible problems. They examined firewall attributes, and cross reference each firewall operation with causes and effects of flaws in that operation, evaluating twenty recognized flaws with existing firewalls. The outcome of their investigation is a set of matrices that demonstrate the distribution of firewall vulnerability causes and effects over firewall operations. These matrices are beneficial in circumventing and perceiving unforeseen hitches during both firewall implementation and firewall testing.

Firewalls can be software or hardware and vulnerability studies in them are classified according to the vulnerabilities in the software, the hardware and vulnerabilities due to misconfiguration (Kashefi, Kassiri and Shahidinijad, 2013). This research will highlight the human factor vulnerability to the list of vulnerabilities.

Software vulnerabilities are flaws that exist in software that can cause a software or system to behave abnormally, triggered by user either coincidently or exploited without hesitation (Stoneburner, et al., 2002, OWASP Organization, 2013and Kaspersky Lab, 2013). It exists due to improper process (Beizer, 1990) and (Piessens, 2002), poor design or fprogramming errors (Alhazmi, et al., 2006), (Aslam, 1995), (Howard, et al., 1998), (Krsul,1998), (Longstaff, et al., 1997), (Moore, 2007) and (Vipindeep, et al., 2005). Off all the identified root causes, programming errors are considered as the most fatal. Programming errors are caused by default due to the programming language like C programming language or due to incompetence programmers in software security (Ahmad, etal., 2011).

Majority of the known vulnerabilities are linked to an improper way of handling the inputs supplied by a user of the system, if these inputs are not properly processed before using them inside the application they can generate unforeseen behavior of the system. For instance, some identified and common vulnerabilities as described by Willy, Amel and Ana (2007) are:

- Buffer overflow: this typically arises with permanent length buffers on occasions when a quantity of data is going to be written outside the boundaries of the existing defined capacity. The new data can corrupt the data of other buffers or processes and could create anomaly in the system. Again, the overflow of the buffer can be utilized to infuse malicious code, and then the execution sequence of the program could be changed in order to execute the malicious code and take control of the system.
- XSS or cross site scripting: typically related to web applications and involves the injection of code in the pages accessed by end users. An attacker can exploit this and use it to bypass access controls, steal identity and perform phishing.
- SQL injection: this is the injection of code to exploit the content of a database. It occurs when user inputs are not efficiently handled which gives the attacker access to sensitive information from the database.
- Format string bugs: this typically occurs when external data is passed to an output function as an argument to format string. The *printf* output function in C language, for instance, creates an output based on the condition of the format string, some directives can write to memory locations, thus the *printf* can be exploited by an attacker to inject malicious code and alter the control flow to execute it.
- Integer overflows: which are of two kinds, sign conversion bugs and arithmetic overflows. The former occurs when a signed integer is converted to an unsigned integer.

In the latter, the result of an arithmetic operation is an integer larger than the maximum integer and it is stored in an integer variable.

2.3 Conclusion

As shown in the literature, vulnerability studies dwell on software or hardware aspects of the information assets ignoring the human aspect. The human factors vis-à-vis Information Technology (IT) have raised interest from the IT fraternity. Lesia and McCauley-Bell (2007) concur that new solutions due to information insecurity have focused on technology alone while the human factor has been limited.

Often, institutions ignore the human factor which is significant in the security framework. Technology is frequently seen as the immediate solution to Information Security problems. Eugene (2005) states that despite the fact that many organizations make use of a high number of technical security controls, they still show a non-proportional number of security breaches; this happens because Information Security is primarily a human factor problem that remains unaddressed.

As far as it is people who use technology it is equally important to invest in the people. Regardless of the robust nature of a security system it will have to depend on people. The increasing reliance on technical solutions alone cannot handle the end users. Schneier (2000) states that it is lack of understanding of security problems to think that technology alone can solve security problems. William and Mitnik (2002) find technological security insufficient and argue that users are targeted when the technological attacks fail. Therefore the human factor is an important factor in assessing vulnerabilities in information assets. This research is geared towards evaluating the human factors that contribute to information insecurity. This study is different from the works in the literature review because it is a significant endeavor to address the human risk of Information system security. It guides on dealing with the complexity of people towards information security.

CHAPTER THREE

METHODOLOGY

The research employed two approaches: experiments and surveys.

3.1 Experiments: Penetration Tests

The purpose of these tests was to find out the vulnerabilities that put data at risk by verifying if the application systems at the institution are exposed to security vulnerabilities that emanate from human errors. The methods used were:

- Social engineering
- SQL injection
- Cross Site Scripting (XSS)
- Brute force attack

3.1.1 Social engineering

Social engineering penetration attempts were performed on employees to find out if they follow security standards and policies. The attack was conducted by developing a phony phish system. The goal of the phony phish system is to send phishing emails that can be used to measure the accuracy of the research.

Components of the Phony Phish System

— HTML Form: This module collects data of the respondents who have the tendency to respond to phishing attacks.

— PHP script: This logs respondents' data to the log file.

— SMTP server: The SMTP server sends a phony email to each respondent. Every email is outfitted with a unique link to the HTTP server.

— HTTP server (Apache): The HTTP server logs respondents' information through a PHP script.

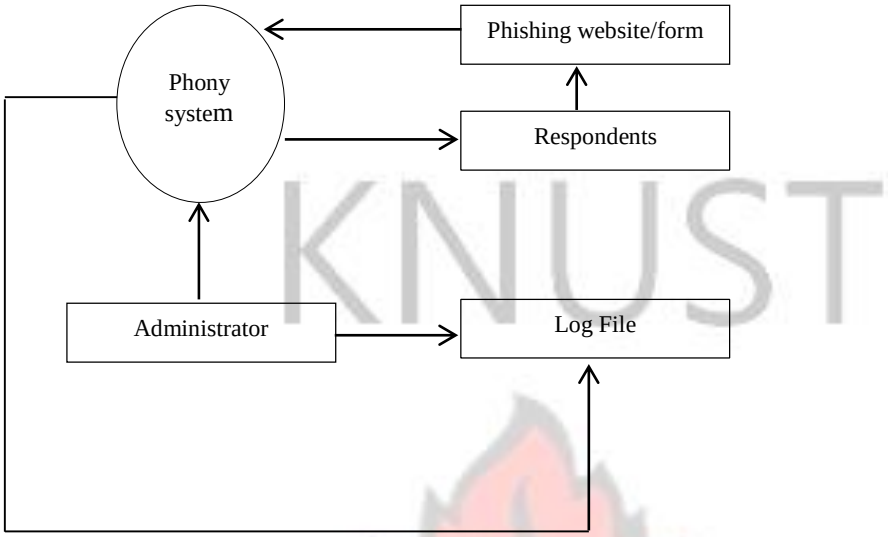

Figure 1: Components of the Phony Phish System

– Phishing attack: To measure the accuracy of the survey as a tool in the investigation of information security, a surprised phishing attacks were conducted. The attack asked respondents to visit a page which then asked them to input given data to continue. The email was formulated as follows:

Hello Dear,

I had your email address from a friend who insisted that you would like this video. I like the video myself and is one of the hilarious video I have seen. You can watch the video from the link below. Have a nice day.

http://bitly.com/1IeLs6s

Regards.

Issa.

The raw data gathered from the social engineering attack is tabulated in table 1.

Table 1: Emails sent in social engineering attacks

No. of emails sent	43

Reachable	Responded	No-Response
	28	8
Non-Reachable	7	

It should be noted that, unlike real phishing attacks, no actual information was collected from the respondents, no software was installed on their systems, and the security of their systems was in no way compromised in this experiment.

3.1.2 SQL Injection

An error-based SQL Injection attack string was formulated to find out if the web application of the institution is vulnerable to attacks. Two criteria were used to detect vulnerability. Firstly, the web app has to allow execution of queries from the url, and secondly, it should show an error for some kind of query or the other. An error shown to the end user is an indication of a SQL vulnerability. A web page that is properly configured shouldn't execute any SQL statement from the end user. However, that is not the case for the web app under investigation. The page that would show before the injection of the SQL statement is shown in figure 2.

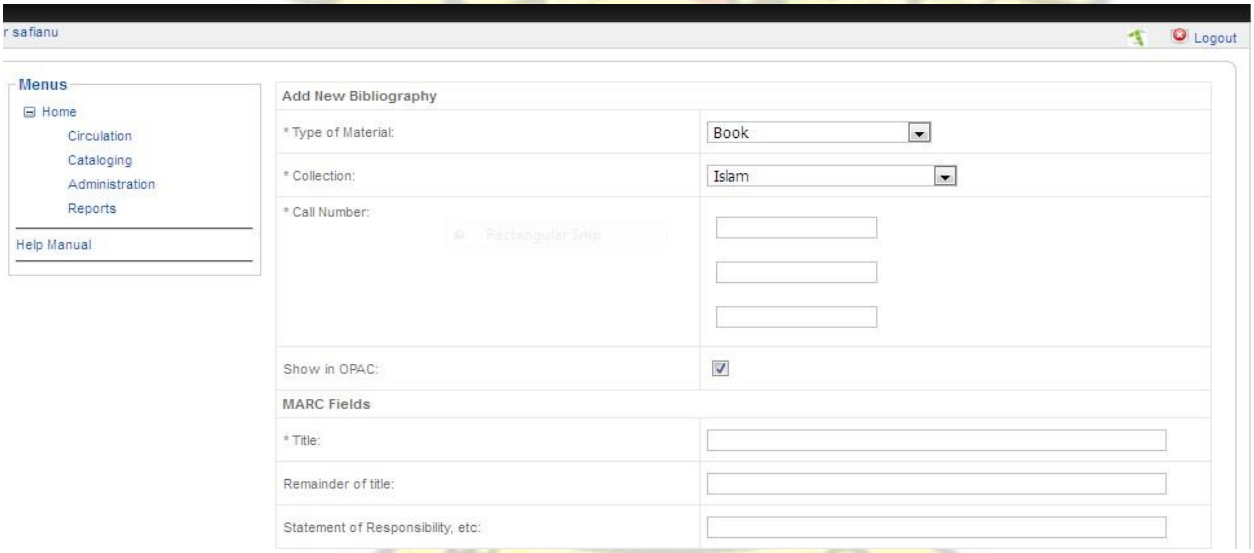

Figure 2: The page shown before the attack

It was found out that the URL of the web app allows queries to be executed. The query included in the URL is: xxx-server/library/iLibAdmin?id=1 or x=1 (I have replaced the web resources

names with “xxx” for security reasons). Since “x=1” is not a valid SQL syntax it won’t execute but will throw an exception (error). The exception that was thrown during the experiment is shown in figure 3. It must be noted that several queries were tested with the URL and all show a kind of error or the other.

Figure 3: SQL Injection Test Result (page shown after attack)

The error message is disclosing information about the internal implementation, namely that there is no column called “x”. This is important because once it is established that an app is leaking SQL exceptions, it can be used for attack.

3.1.3 Cross Site Scripting (XSS)

Cross Site Scripting vulnerabilities most often happen when user input is incorporated into a web server's response (i.e., an HTML page) without proper validation. To do this, a java script (<script>alert('123')</script>) was injected in the url. The page before the attack and the result after the attack are shown in figures 4 and 5 respectively.

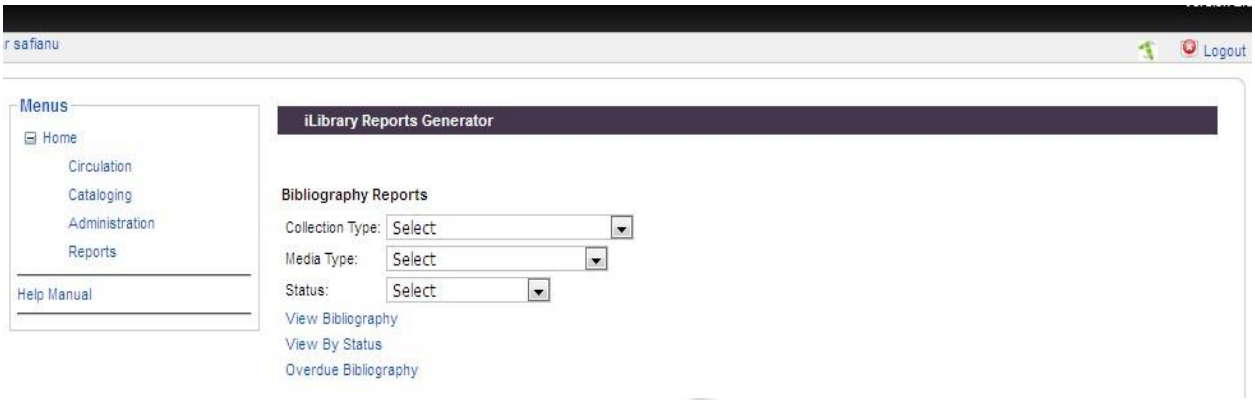

Figure 4: Page before XSS attack

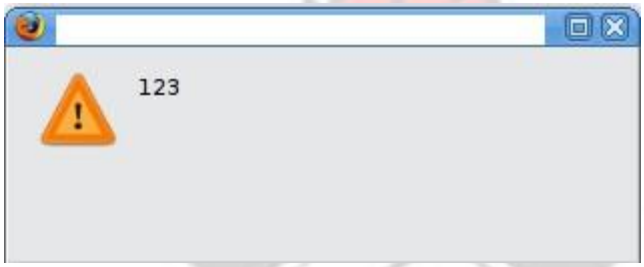

Figure 5: Cross Site Scripting (XSS) test result

This indicates that there is an XSS vulnerability because the application echoed back the JavaScript payload (<script>alert('123')</script>) on the page returned by the server.

3.1.4 Brute Force Attack

Brute force attempts were made to reveal some of the human factors that can make data vulnerable to attacks. To do this the admin webserver interface was accessed. OWASP DirBuster, which is an open source (third party) software, was used for the test. The admin xxxserver/xxx/admin folder which contains the Apache server was found to be running on port 81. When the main URL of the site was accessed only a blank page was displayed. To reveal common folders and files of the system, an enumeration scan was made in order to see the folder structure.

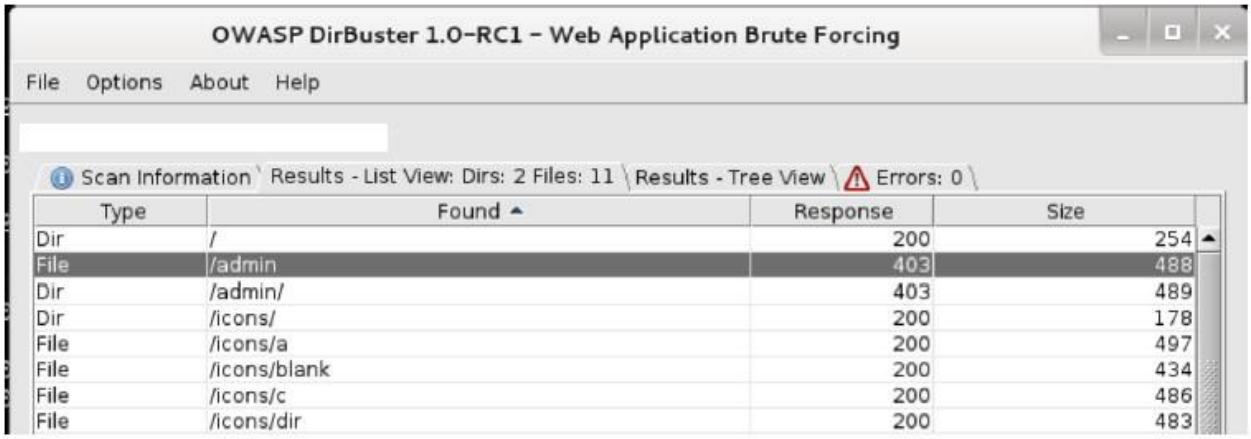

Figure 6: Scanning the xxx-server/xxx/admin reveals the webserver's folder structure. The scan results revealed, among other Apache default files, an "/admin" folder. The folder is password protected and can only be accessed after authentication as shown in figure 7.

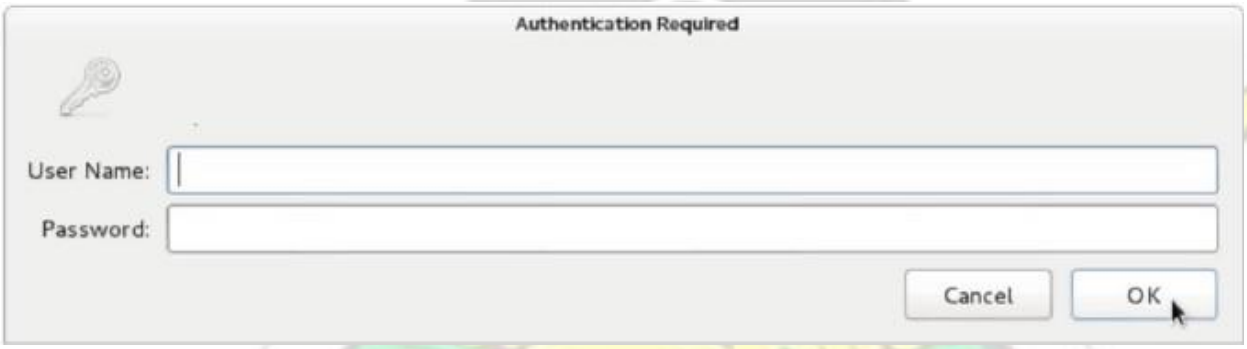

Figure 7: The "admin" folder is password protected.

To set up a brute force attack on the system, a compilation of the contents of the web app was collated to form a dictionary file. The dictionary contained 66 raw words. These words were permutated and substituted severally to produce a final dictionary file of 3,240 words. With the username "admin", the dictionary file was used to attempt to break into the protected section of the site.

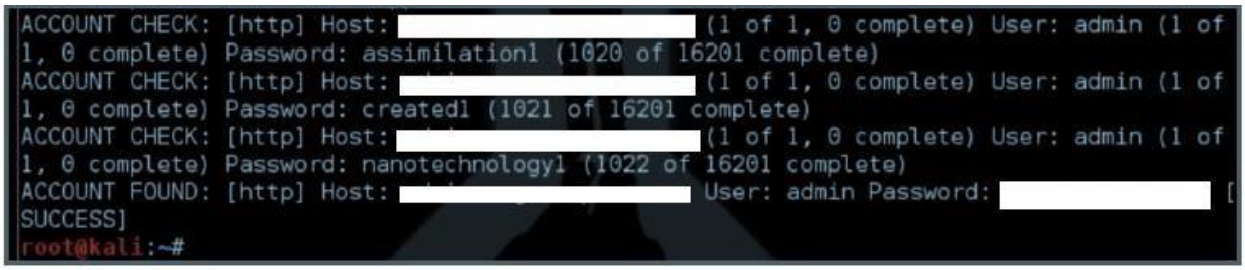

Figure 8: Dictionary words being used to reveal the password to the "admin" folder A password for the admin file was revealed during the brute-force attack. These credentials were leverage to successfully break into the system and access the protected admin file.

3.2 Surveys

A smoke-screen approach was used in the survey as it is more effective to capture respondents' security awareness if they are not aware of their awareness being assessed. This is because the respondents might act differently if they knew that their awareness was being assessed. Thus, the survey was entitled "Effectiveness in student-staff relationship". The title was chosen so that the respondents would not realize that the survey was about information security.

The survey comprised of seven scenarios. Two of the scenarios had general attributes which were used as diversion from the hidden subject. The other five questions had the real purpose of evaluating respondents' propensity to:

- Accessing a link from unknown sender
- Responding to requests to install programs form unverified person
- Sharing keys to wireless network to visitors
- Sharing username and password with colleagues
- Using weak or strong password

The data collection was started by the researcher sending out an email and informing respondents about a study in "student-staff relationship" and encouraging them to answer a survey related to this study.

3.3 Interviews

To augment data to the questionnaires, ten IT professionals were interviewed. The IT professionals work in various roles in the IT industry. Their views were solicited on the practices and behaviours (human factors) that employees exhibit that can make data and information vulnerable to attacks and theft. The interview was unstructured which allowed open responses.

The responses were transcribed and analyzed.

3.4 Entropy Formulae

The entropy formulae was used to measure the password strength of respondents. The entropy formulae states that $E=\log_2 (x)*L$ where E is the entropy, x is the pool of characters used in the password and L is the length of the password. An $E \geq 80$ bits signifies a strong password and $E < 80$ bits signifies a weak password. The entropy was calculated by looking at the pool of characters used by respondents.

CHAPTER FOUR

ANALYSIS OF RESULTS

4.1 Introduction

This chapter analyses the data collected from the survey and experiments.

4.2 Results analysis from survey.

Forty Three (43) emails were sent to the respondents (this is the number of staff who frequently use information systems). The emails were fused with Google form link that requested the respondents to provide answers to the survey entitled "Effectiveness in student-staff relationship". This is a smoke-screen title and this was chosen because it is more effective to capture the respondents' security awareness if they are not aware of their awareness being assessed. This is because the respondents might act differently if they knew that their awareness was being assessed. Thus, the survey was entitled as such. The title was chosen so that the respondents would not realize that the survey was about information security. The survey investigated respondents' tendency to:

- Accessing a link from unknown sender
- Responding to requests to install programs form unverified person
- Sharing keys to wireless network to visitors
- Sharing username and password with colleagues
- Using weak or strong password

The email could only be delivered to 36 respondents out of 43, as 7 recipient email addresses were unreachable. Out of the 36, only 28 responded. Hence, the total number of participants in the survey is considered to be 28 representing 65.11% response rate.

When the question "Have you ever responded to an online request to provide your account or profile details? Was posed to the respondents, 21 (75%) said Yes, whilst 7(25%) said No. With

regard to the infection of respondents' computer by malicious software, almost all the respondents (24(85.71%)) answered in the affirmative. This attitude of respondents can put data and information at risk in that hackers can use this vulnerability to retrieve sensitive information from them.

Another study of information security of respondents was on generation and usage of the password. Three variables were used in determining this part of security awareness. The variables were:

- Characters used by respondents to generate password
- How long in characters of generated password
- Rate at which passwords are changed

The responses to the above variables are summed up in figures 9, 10 and 11.

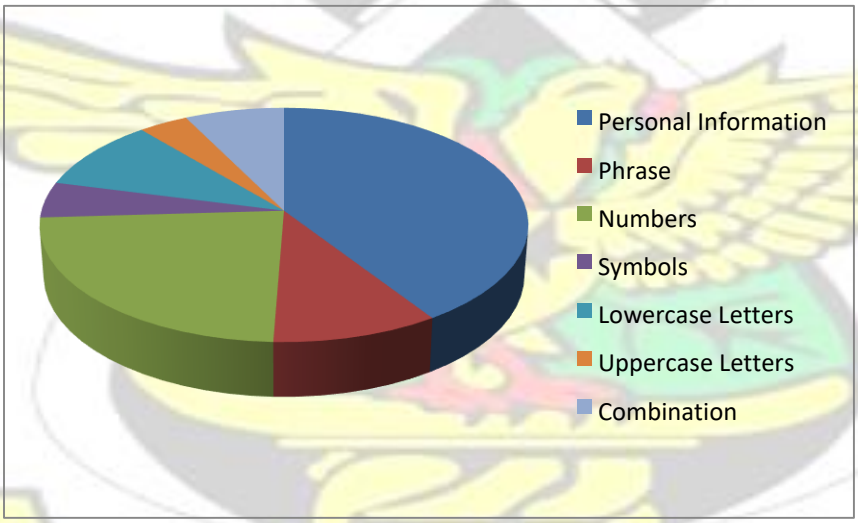

Figure 9: characters used by respondents to generate passwords.

As shown in figure 9 above, 11 (39.2%) of the respondents said they use personal information such as name, date of birth, place of birth, address, etc. to generate password. 3 (10.71%) said they use phrase, 5 (17.85%) use numbers, 2 (7.14%) use symbols, 3 (10.71%) use lowercase letters, 2 (7.14%) use uppercase letters, while 2 (7.14%) use a combination of the above.

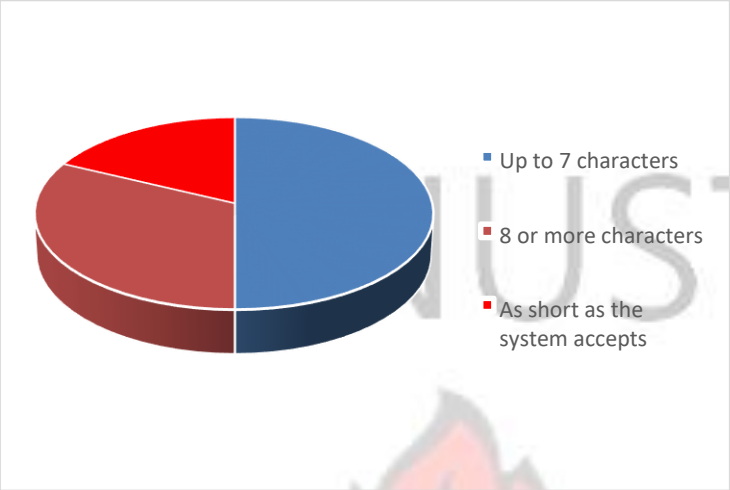

Figure 10: Length of generated passwords

Figure 10 shows that 14(50%) of the respondents use up to seven characters to generate their password. 9(32.14%) use eight or more characters whilst 5(17.85%) said their passwords are as short as the system allows.

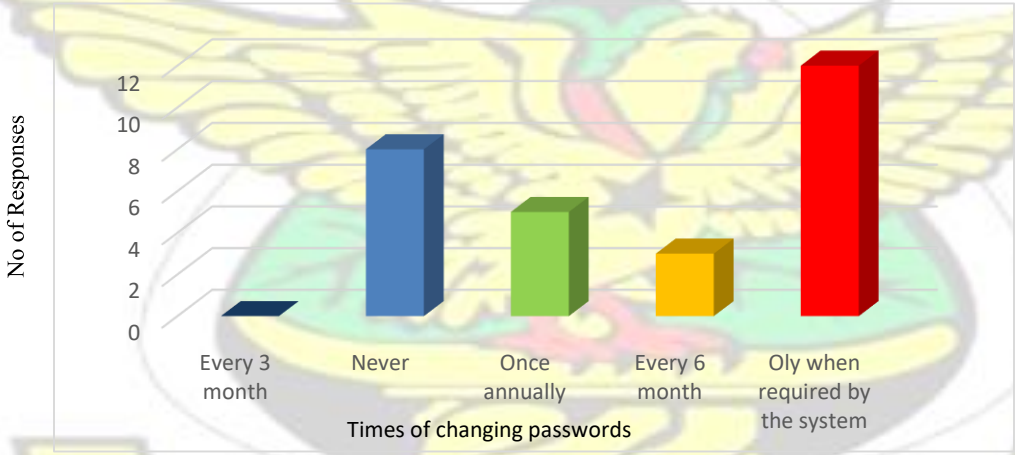

Figure 11: Rate at which respondents change their passwords

As shown in figure 11, 12(42.85%) of the respondents change their passwords only when the system requires them to do so, 8(28.57%) never changed their passwords, 5(17.85%) change their password once annually, 3(10.71%) change it every six months, and none change it every three months.

Related to the above, a question as to whether respondents would reuse the same password for several accounts was asked. 19(67.85%) of the respondents said Yes, while 9 (32.14%) said No.

When the question "if you were not able to change a password that is difficult to remember, would you write it down?" was posed to the respondents, 21(75%) said yes while 7(25%) said No.

Having a strong password is one of the ways to protect information. As shown above, respondents use guessable data to formulate their passwords. Their password can be described as weak (this has been calculated and can be seen further below). The significance of this is that their accounts can be broken into easily using brute force techniques thereby putting data at risk.

The following tables summarize the remaining responses given during the survey. **Table 2:** Other responses from the survey

Variables	Yes	No	Total
Preventing others from watching when typing password	19 (67.85%)	9 (32.14%)	28 (100%)
Opening email or attachment From unrecognized address	18 (64.28%)	10 (35.71%)	28 (100%)
Sharing username or password with someone else	7 (25%)	21 (75%)	28 (100%)
Entering credentials on website whose address does not start with "https"	17 (60.71%)	11 (39.28%)	28 (100%)
Installing updates from unverifiable sources	16 (57.14%)	12 (42.85%)	28 (100%)

As shown in table 2, out of the 28 respondents, 19 (67.85%) said they would prevent others from watching them whiles typing their passwords into the system while 9 (32.14%) said they wouldn't mind others watching them when typing their passwords. 18 (64.28%) of the

respondents indicated that they would open an email link or attachment from unrecognized email addresses. However, 10 (35.71%) would do otherwise.

A question was asked as to whether respondents would share their usernames and passwords with friends and colleagues at work place or not. As shown in table 2 7(25%) said they would share their login details while 21(75%) responded in the negative.

17 (60.71%) of the respondents said they would enter their login details on a website whose address does not start with https and 11 (39.28%) said no. Table 2 also shows that 16 (57.14%) of respondents said they would install unanimous security updates on their computers and 12 (42.85%) said No.

The implication of these attitudes of respondents is that a third person can have access to their log in details.

Data was also gathered on whether respondents log off their computers when not in use. This is shown in table 3.

Table 3: Responses on logging off unattended computers

Variable	Yes	%	No	%	Total
When leaving work premises	11	39.28%	17	60.71%	28/100%
When attending office meeting	9	32.14%	19	67.85%	28/100%
When using the wash room	5	17.85%	23	82.14%	28/100%
When closing from work	25	89.28%	3	10.71%	28/100%

As shown in table 3, 11 (39.28%) of the respondents will log off their computers when leaving the work premises, 17 (60.71%) will leave it idle. 9 (32.14%) will sign out of their computers when attending office meeting while 19 (67.85%) will leave them unattended to. 5 (17.85%) will log off their systems when visiting the wash room and 23 (82.14%) will do otherwise. 25 (89.28%) will sign out of their computers during closing hours while 3 (10.71%) will not sign out.

One of the actions that can put information at risk is not logging off unattended computers. The repercussion of this attitude is that one can have access to these computers and the data and information contained in the computers at the detriment of the main user.

When the question "have you helped a visitor to access the wireless network or shared the password with them before?" was asked 13 (46.42%) said Yes and 15(53.57%) said No.

4. 3 Results from Experiments

4.3.1 Social Engineering

To measure the accuracy of the survey a phony phishing system was developed to test respondents' information security. Three of the survey variables were experimented and these were:

- Respondents tendency to install programs requested by an unknown person
- Respondents' tendency to give away username and password
- Respondents' password strength

4.3.1.1 Respondents tendency to install programs requested by an unknown person Out of the 43 email messages sent through the phony phish system, 25 respondents clicked on the link within the email message and visited the experiment website. The experiment website was closed over a specified period of time even though visits to the website were still being recorded therefore the true percentage of unique visits is likely to have been higher. Figure 12 shows the number of responses by week.

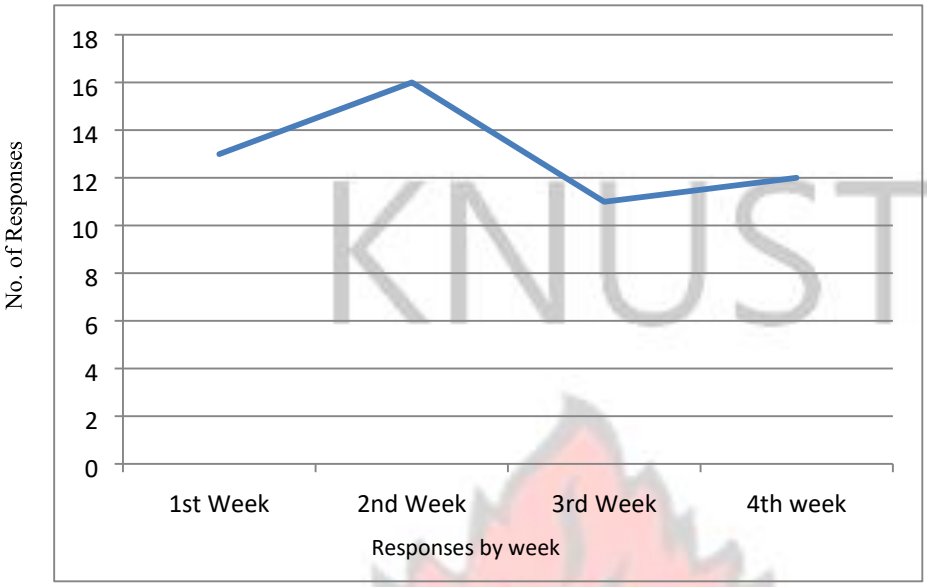

Figure 12: Number of responses to the phishing email by week.

Majority of the respondents who followed the link and visited the first page of the website also clicked the 'continue' button to proceed. This is shown by the number of messages that were collected in the log file. This asserts that the respondents did not mistakenly click on the first page, as making the same mistake repeatedly is improbable.

The significance of this is that respondents are likely to respond to phishing emails and attacks from hackers.

4.3.1.2 Respondents' tendency to give away username and password

Out of the 43 email messages sent for the second attack, 19 respondents followed the link within the email message and visited the experiment website.

The attack was performed to see if respondents will click on a link that asked them to enter their credentials (in this case they were asked to enter a code embedded in the experiment page).

Unlike real phishing attacks, no actual information was collected from the respondents. The research was interested in finding out whether they are likely to click on a link that asks them to update their log in details.

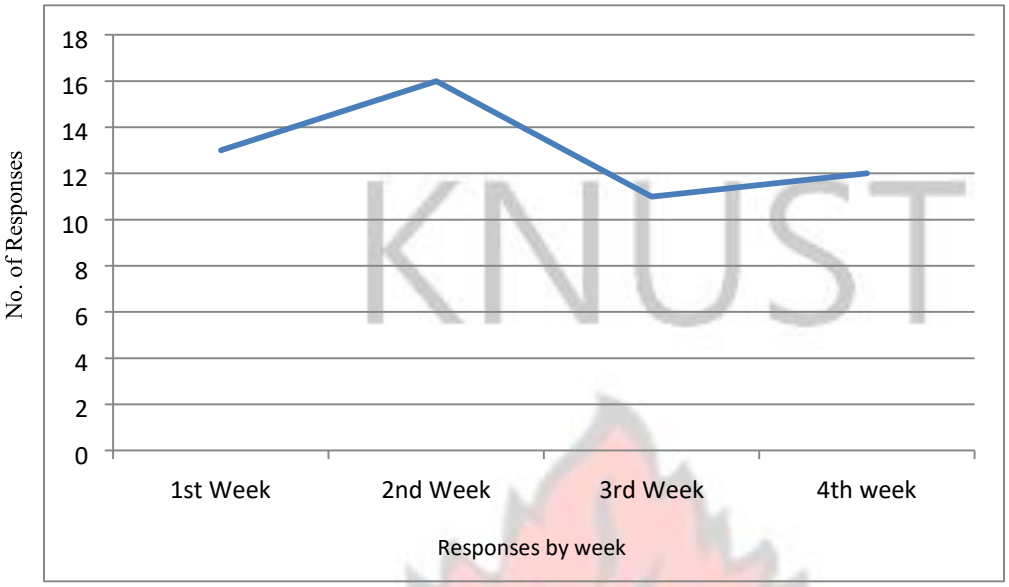

Figure 13: Weekly number of the respondents which clicked on the link and entered the code

The implication of this is that respondents are likely to give away their passwords to attackers and the repercussion could be great.

4.3.1.3 Measuring respondents' password strength

One of the issues in information security vulnerability is in relation to password. Data on the kind of characters respondents used for their password were collected. This will help in measuring the strength or weakness of respondents' password as having a weak password can put an information system vulnerable to attacks.

To measure the password strength of respondents, the entropy formulae $E=log_2 (x)*L$ was used. Where E is the entropy, x is the pool of characters used in the password and L is the length of the password. An $E \geq 80$ bits signifies a strong password and $E < 80$ bits signifies a weak password. Password entropy is the measurement of how predictable or unpredictable a password is. In other words, password entropy predicts how difficult a given password would be to crack through guessing, brute force cracking, dictionary attacks or other common methods. The entropy was

calculated by looking at the pool of characters used by respondents. The study revealed that respondents use a phrase, numbers, lower case letters, upper case letters, or a combination of them to generate their passwords. This will give us a possible pool of characters as shown in table 4.

Table 4: Pool of possible characters for generating password

Type	Pool of possible characters
a-z	26
A-Z	26
Numeric	10
Symbols	21
Combination (all key board characters)	94

On average, respondents use up to seven (L=7) characters to generate their password. In computing for E in various combinations the following results were derived:

A password generated from the pool of lowercase characters only: $E=\log_2 (26) *7= 32$ bits

A password generated from the pool of alphanumeric characters: $E=\log_2 (36)*7=36$ bits A password generated from the pool of alphanumeric and symbols: $E= \log_2 (57)*7= 40$ bits

A password generated from the pool of all the keyboard characters: $E= \log_2 (94)*7=45$ bits. Therefore, the overall strength of password of the respondents can be described as very low since the length of password of majority of the respondents is 7 which will give an $E< 80$ bits. To have an $E \geq 80$ bits security a password will need at least an L=13 from the pool of all keyboard characters.

4.3.2 SQL injection

An error-based SQL Injection attack string was formulated to find out if the web application of the institution is vulnerable to attacks. Two criteria were used to detect vulnerability:

- Does the web app allow execution of queries from the url?
- Does the server throw back exception (error) to the browser?

An invalid SQL query was included in the URL of the system and run. The query included in the URL is: “xxx-server/xxx/?id=1 or x=1” (I have replaced the web resources names with xxx for security reasons). Since “x=1” is not a valid SQL syntax it won’t execute but will throw an exception. It was found out during the attacks that the system shows an error for some kind of query or the other to the end user. An error displayed to the end user is an indication of a SQL vulnerability and hence data vulnerability. This could be classified as human factor because the database system was not configured properly by the developers.

Figure 14: Exception (error) thrown back to the end user

4.3.3 Cross Site Scripting (XSS)

Cross Site Scripting (XSS) is a web hacking method where an HTML or Javascript can be injected on the web-page. This attack can be done by submitting queries into text boxes or simply in the URL. The result will be the website reads the query and executes it. XSS is a very powerful method, it can be used to steal someone’s cookies or it can be used to manipulate people to download a virus.

A basic JavaScript was injected into the system’s URL in order to test if this vulnerability persist in the system. The result of the injection is shown in figure 15.

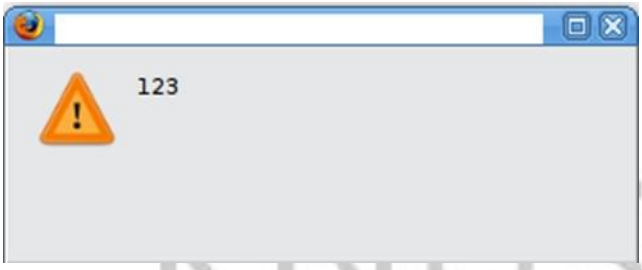

Figure 15: Cross Site Scripting test result

This indicates that there is an XSS vulnerability because the application echoed back the JavaScript payload (<script>alert('123')</script>) on the page returned by the server. This could also be attributed to human factor because the system lacks a filter that checks for malicious (dangerous) content, like HTML and Javascript. A filter can block the script and prevent it from executing.

4.3.4 Brute force attack

The experiment also found out that the system is vulnerable to brute force attacks. A brute force attack is a trial-and-error method used to obtain information such as a user password or personal details. In this attack automated software (OWASP DirBuster) was used to generate a large number of consecutive guesses as to the value of the desired data.

To do this, the server's port number was identified (that is port 81) and then a quick enumeration scan of the system to reveal common folders and files was made. This displays the structure of the folders in the webserver which helped in accessing the admin folder. A targeted brute force attempt against this system was prepared with a custom dictionary words of 66 which were permutated severally to form a final dictionary file of 3,240 words. Along with the "username" the dictionary file was used to attempt a break into the protected part of the system. The bruteforce attack revealed a password for the admin user. The password was leverage to effectively gain unofficial entrance to the protected part of the system.

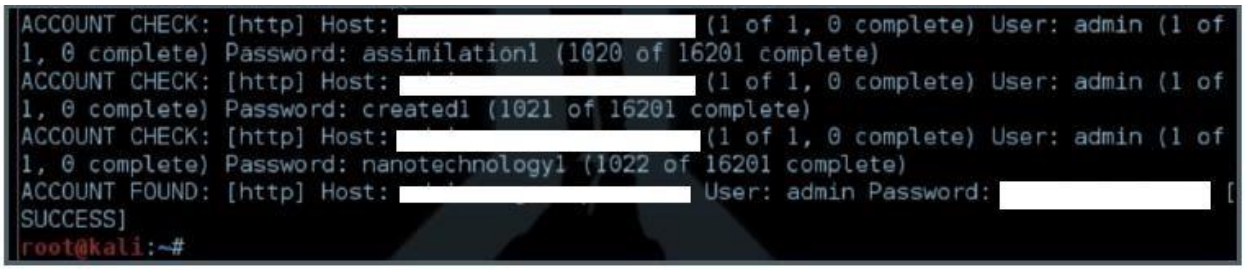

Figure 16: Using dictionary word to discover the password to the "admin" folder Human factor can be linked to the successful break into the security of the system because the system allows several attempts of logins. The system should have put a mechanism in place that locks users out of the system after three or two attempts of logins.

4. 4 Results from IT Professionals

To augment data gathered from the questionnaire, ten IT professionals were interviewed. The IT professionals work in various roles which include system administration, cyber security experts and database administration.

Frank Addai (personal communication, August 15, 2014), a systems administrator, laments the increase in client-side attack as a result of the rapid growth of social networks which mostly come from the end user side. The attack normally arises when the victim trusts the contents or files provided by the attacker which appears to be legitimate. He advises that security mechanisms have to be put in place to check on these attacks.

He alludes that, usually, the first line of defense of such attacks are network security devices like IDS/IPS systems, Firewalls and Proxies. Technology has improved so much so that it allows these devices to offer robust inbound security. However, these devices alone cannot stop all traffic because specific services, such as inbound email and outbound internet access, are critical to the business and have to be granted access.

Micheal Terpor (personal communication, August 15, 2014), a cyber-security expert, adds that an attacker will always find a loose end first in his quest for data access. Security put in place at the edge of the network is the first obstacle for the attacker which is very difficult to be bypassed these days. Email and social networks are the only viable routes into the network. Once the attacker is able to communicate with workers through these routes, then the firewall has just been defeated. Workers' desktop are usually less harden than other computers connected to the network and the fact that users tend to run vulnerable applications on their systems makes them ideal targets allowing the attacker to have access to their systems and consequently the entire network.

Iddriss Ahmed (personal communication, August 15, 2014), considers the issue of inconsistency in privacy settings and indicates that lack of consistence in privacy settings opens the door for attackers to access the data they need. Attackers usually profile their victims by gathering information on them through the internet especially on social networks. Personal and professional networks offer a chunk of information for they are the platforms where victims regularly update their status. Often end users secure their privacy settings on a network, and yet again they are careless with what they publish online. The attacker eventually profiles the published information and use it to craft his attack.

He further indicates that one of the actions that can compromise security is by connecting office devices to public networks. When a device is compromised, an attacker can access its sensitive information and the device can be used as a new entry point to the corporate network. If a portable device is connected to a corporate network, other devices connected to that network are potentially accessible from the portable device. As many workers connect their mobile devices to the home network, which has relatively loose security, could expose their devices to attacks, as the devices would no longer be protected by a more secured corporate network. He stresses that when these

devices are inactive, silent attacks could be launched on them so that when they are connected to the corporate network the real attack will be unleashed since they are already associated with the network and will be considered as trusted devices. Security on portable devices has improved over the years even though there are still rooms for improvement. He advises that caution should be exercised when portable devices such as smart phones are being granted access to a corporate network.

Osabutey Amin (personal communication, August 25, 2014) outlines some mistakes system administrators make that can put data at risk which include the lack of a well-established personal security policy. He asserts that quite a number of system administrators don't follow established standards on personal security like network security, arbitrary system's software updates and chaotic application of new patches. He states that the well-established companies fall short of this especially on their reluctance to patch their systems when new bugs are discovered.

His views are that at times the system administrator is not aware of the latest vulnerabilities discovered in a software or hardware, which are potentially dangerous to the organization's network. Security is a continues effort that demands persistent evaluation and monitoring. Even if the administrators are not well versed in security matters they should continue to abreast themselves with current methods on security in order to protect and secure their networks. He recommended the following for improving the security of terminals:

- Terminals and offices must be physically protected to keep at bay the risks of malicious "snoopers" walking around the workstation in order to have access to the terminal.

- Administrators must set up a logout mechanism so that once the system detects inactivity for a set of time it will be logout automatically. In this way, the system will be protected once it detects that there no one in front of the keyboard.
- Taking records of login details and IP information on paper should be discouraged.

Enoch Asante (personal communication, August 15, 2014) presents two security issues that can put data at risk. These, he listed as, failing to monitor the logs and running extra and unnecessary services and scripts. He stresses that if the system's logs are monitored periodically it can mitigate risky intrusions. Monitoring the system's logs helps in understanding the common vulnerabilities attackers are scanning and might help in tracing back the attacker.

He adds that running extra and unnecessary services and scripts can also expose data. Using the organization's devices and network as a platform for testing various scripts and services is one of the major mistakes committed by some administrators. When these scripts are run on the network, especially on the server, it may result in new entry points for attackers. He recommends that new scripts be tested on isolated computers which are not connected to the company's network. This could limit the odds of attackers discovering the scripts.

Bismarck K. Inkoom (personal communication, August 15, 2014) highlights some of the mistakes end users make that put data at risk. He states that violating the institution's security policy could open the door for attackers to take advantage**.** Some of the issues outlined in security policies are responsibilities of identified staff who have access to critical system information. This should be considered as indispensable part of any company's security framework because it provides the staff with ways to secure the systems while using them. When these policies are violated, sensitive systems and information could be compromised.

The second mistake that he highlighted was end users moving critical data to their personal computers at home which could be compromised to attackers. This behaviors can turn all of the security measures in an institution into a totally hopeless process. Workers tend to move a pending assignment to their personal devices so they could work at home. This could expose the forwarded data to attackers as the home devices are less secured. With the advent of mobile technology, a lot of tasks are increasingly distributed which broaden the potential risk for data loss. Moving files from computers at the work place to a home computer that is not secured to IT's standards, using private devices that are not as safe as company devices, discussing about sensitive business issues in the public, and lack of usage of security guard when working afar can lead to information theft. Workers also fall short in safeguarding portable devices such as laptop computers and storage gadgets. He recommends that if workers intend to move data to their personal devices it is important that security audit of the devices are made regularly to ensure that they are protected from attacks.

Another end user mistake, as alluded by Teigo Eshung (personal communication, August 05, 2014), is writing down login data. Memorizing login details is an issue that troubles users. To avoid this, users tend to write it down and place it under the keyboard, in their wallet, or anywhere else in the office which could increase the chance of security breach. Many end users of information systems fail to adhere to basic security protocols such as logging out of a computer and using a password which is quite surprisingly as he alluded. Workers leave their computers logged on and unattended to when they are out of the office.. Again, employees tend to leave their unlogged-off laptops on a desk overnight which is risky to data. Yet again, system login details are stored on devices or written down by employees on their desktop which could be discovered by others.

He reiterates that failure to adhere to security measures is a fine opening for attackers. These could open the door for insider attack. For instance, an unlogged-off system with attached password left by a worker could be used by an intruder to effect certain changes on the system or have access to sensitive business or personal data of the worker.

He adds that downloading from untrusted web sites can also compromise security. Workers tend to misuse the privileges given to them for internet access by downloading from unsafe websites which could endanger data security by spreading malicious programs over the company's network. The malicious programs(virus, trojans, worms could cause serious infection which can affect the functionality of the organization.. He recommends that downloads should be controlled by the IT department

Solomon Baneseka (personal communication, August 05, 2014) asserts that ignoring physical security issues can create serious threat to data. Possessing an understanding of various physical security problems could help in securing the network and consequently protecting sensitive data. He stressed that some workers are irresponsible and are security unconscious when using the company's computers. They often leave their computers unattended and without password.

Justin Kobla (personal communication, August 29, 2014) asserts that despite the security policies, procedures, and tools being used in organizations, employees engage in risky behaviors that can put corporate and personal data at risk. He highlights some of the risky behaviors which include:

- Unauthorized application use which can lead to security failures.
- Abuse of privileges for business devices: when staff share office computers and devices without control.

- Unofficial physical and network access: he stated that he has dealt with employees intruding on parts of the company's network.
- Movement of files between office and home computers by employees.
- Improper handling of log-in credentials through sharing of passwords with co-workers.

He suggests that at times financial reward is one of the reasons for putting data at risk. And t is because it is inexpensive to use the computer at the work place for a personal business which could lead to outsiders having access to corporate information. He opines that, sometimes workers are the threat themselves. If a worker is discontented with his job, displeased with his superior, or he is bitter for any reason, he can become a threat to the institution by intentionally deleting or revealing data to competitors.

To decrease data insecurity, he recommends that it is necessary for institutions to incorporate security as part of work culture and to constantly do risk assessment of all devices connected to the network and the applications installed on them.

Erick Asema (personal communication, August 15, 2014) concurs and states that employees who install unofficial software or applications on their office computers and devices could place essential business data in danger. He indicates that the most common unauthorized applications used by workers are email applications and social networks which could create avenues for hackers to steal both personal and company information because often these applications are not checked and do not use unique security standards.

He also laments that some employees undermine IT security policies by consciously using office computers carelessly. For instance, some employees may change security settings of their office computers and share office devices and sensitive information with outsiders. Some even go further

by sidestepping IT settings to download music and other files. He has had instances where workers disclosed that they had shared office devices and information with friends and family without official approval or supervision. These acts could lead to leakage of trade secrets to competitors or disclosure of sensitive data to hackers that could cause serious threats to company security and prosperity.

He opines that security threat to data are changing and much of these come from hacking through the internet. Through exposure of company's network on the internet, workers are leaking data even with the best efforts to stem it.

As businesses become mobile and operate online, there is virtually no solution to the leakage due to the ignorance, non-compliance to security, and a simple lack of caring by employees. It is wrong to put too much trust in technology alone because the best security technology put in place is not enough to produce a good security measure without groundwork on security education and policies. He suggests that, in order to have a good security framework, institutions should start by assessing workers behavior on security and then offer training if need be before thinking about investing on security technology.

CHAPTER FIVE

FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter represents an elaboration on the research findings. It provides an assessment of the findings on the basis of which conclusions could be drawn.

5.2 Human factor vulnerabilities in information security

The following are human factor vulnerabilities that emerged during the survey and experiments. These threats and vulnerabilities include acts performed without intent or malicious purpose by an authorized user (respondents). When people use information systems, sometimes improper usage happens. Inexperience, improper training, and the making of incorrect assumptions are just a few circumstances that can cause these vulnerabilities.

i. **Clicking on links from unverified senders**

Clicking on links from unverified sources can lead to security breach. It is one of the ways employed by phishing attackers and social engineers to persuade another person to give them the information that they want. This is very effective as it can utilize strategies that bypass computer technology. Therefore, organizations that use secure protocols and procedures and have secure hardware and software are equally vulnerable to these attacks as those organizations that lack technical and computer security.

The study shows that quite a number of the participants (49.52%) would followed a link that requested them to change their credentials while 42.85% of the respondents would follow a link that requested them to download updates. It is interesting to note that majority of the respondents (90.21%) said they would enter their login details on a website whose address does not start with “https”.

Phishing and social engineering is one of the most effective routes to stealing confidential data from organizations. These attacks are a growing threat because attackers' primary motivation is stealing sensitive data or financial information or extracting trade secrets. Furthermore, by attacking the right people, attackers can gain a grip in the corporate network, then use it to exploit sensitive information. Phishing and social engineering attacks are more challenging to manage

since they depend on human behavior and involve taking advantage of vulnerable people. Businesses and individuals today must utilize a combination of technology solutions and user awareness to help protect sensitive information.

ii. **Lack of strong password and inappropriate password and login/logout procedures**

The usage of a weak password, writing down and sharing of passwords with others, and reusing the same password on different systems are some of the bad practices that could put data to risks. Passwords are to protect data from access from unauthorized individuals both internally (other employees) and externally (hackers). If the password is compromised, the security of the system is at stake.

The study found out that quite a number of the respondents engage in practices that could compromise their passwords. It was established that 46.73 % of the respondents change their passwords only when the system requires them to do so and 31.52 % never changed their password.

On password strength, it was found out that 35.86 % of the respondents use up to seven characters to generate their password. And 29.34 % said their passwords are as short as the system allows. Again, 35.86 % of the respondents said they use personal information such as name, date of birth, place of birth, address, etc. to generate their password while 20.65 % use only numbers. Also, 90.21 % of respondents said they would write their password down when it is difficult to remember.

The password strength of respondents was measured using the entropy formulae $E=log_2 (x)*L$. Where E is the entropy, x is the pool of characters used in the password and L is the length of the password. An $E \geq 80$ bits signifies a strong password and $E < 80$ bits signifies a weak password.

On average, respondents use up to seven (L=7) characters to generate their password. Therefore, the overall strength of password of the respondents can be described as very low since the length of password of majority of the respondents is 7 which will give an E< 80 bits.

Admittedly, complexity of passwords is one of the biggest issues that is being grapple with in the information security industry. Ideally, a password should be difficult to guess which also implies that it should not be a phrase or word or a number such as birth date or telephone number that can be associated with the user easily. However, the password should be created with something the user can easily remember. In other words, it should be short or commonly associated with something the user can recall.

However, that does not mean that people should have a password which can be guessed easily. Perhaps a "passphrase", which is friendlier, should be adopted by end users. A "passphrase" is a series of characters, typically longer than a password, from which a virtual password is derived. For example, while a typical password might be "45dooske," a typical passphrase can be "MayTheLordBeWithYouAlways," which can also be represented as "MTLBWYA."

iii. **Leaving computers unattended to**

Computers which have been left idle and unattended to can pose a threat to data as do other threats. This gives room to unauthorized accesses which can facilitate access to sensitive data and email messages.

This study shows that majority of the respondents (55.43%) will leave their computers idle when leaving the work premises. Again, majority of them (67.39%) will leave their computers unattended to when attending meetings and 81.52 % will not log off their computers when visiting

the washroom. These actions put data at risk especially the risks of insider attacks associated with employees leaving their PCs unattended with active sessions running. A significant number of unauthorized access events may occur when someone sits down at another user's computer.

Threats to unattended computers can be in forms like illegal access to employee's data like salary information; unlawful access to sensitive business information to the level of changing that information (This could be in a form of concealing up a fraud or increasing bonuses or commissions by changing sales numbers). Another threat is the tendency to sidestep approval processes and access levels by accessing a superior's computer. Institutions are protecting their systems and workers against physical security threats, but ignoring the very real threat that exists from something as basic as an unattended PC. Sending emails in another person's name could have huge consequences .A simple thing like that could lead to security breach like access to customer information. These threat can be avoided if employees are educated to log out or lock their devices when they leave their desks. Moreover, a session timeout could limit the risk to unattended computers.

iv. **Connecting to networks outside the corporate infrastructure**

Connecting to a private or a public network other than the corporate network infrastructure can pose a serious threat to data when the device used to connect is compromised. A device which has been compromised could be used as a gate way to a corporate infrastructure. Workers who connect their mobile devices to the home network could expose their devices to attacks, as the devices are outside the perimeter of the more secured corporate network. One of the IT personnel interviewed states that attackers could launch a silent attack against any device connected outside a corporate's network when it is inactive pending the device to connect back to the corporate network. This

allows the attacker to gain access to the network from the inside because the network will consider the devices as trusted ones as they are already associated with the network.

v. Lack of well-established personal security policy and inconsistency in privacy settings The lack of consistence in privacy settings gives attackers room to operate. End users are found to be strict on security on one network but are careless on what information they put online. Two of the IT professionals interviewed lament on this attitude, especially the behaviours of system administrators. Personal and professional networks where the workers freely and frequently update their status can offer a chunk of information for attacks. Attackers can gather this information and use it to sketch their victims, with the most popular source for such search being the Internet, especially the social networks.

One of the cyber-security experts alludes that email is one of the routes attackers use to access a network since breaking the security perimeter is much harder today. When users use the corporate network to send and receive emails they are putting the network and data at risk. As workers connect to both the private (corporate) and public (internet) networks, their computers are often less secure and the fact that they run unauthorized applications like emails and outdated software on their computers makes them the perfect targets, allowing the attacker to access their computers and largely the corporate network.

Two of the IT professionals interviewed stressed that some workers are irresponsible when using the institution's computers. They often leave their computers unattended and without proper password. All these behaviour make data and information vulnerable to attacks.

vi. Unauthorized application use

Unauthorized applications used by users in corporate networks can compromise security of these networks. The unauthorized applications are mostly downloaded from malicious web sites. Workers abuse the opportunity given to them for Internet access by downloading from untrusted sites which endanger security of data. All the IT professionals concur that malicious programs can be spread over corporate network when files are downloaded from unknown and untrusted web sites. This could cause serious security breach. Business and worker's personal information can be at risk when unofficial applications are used on business networks. The study revealed that the frequently used unauthorized applications are email and social networks. Workers could lose sensitive data through negligence and hackers could steal data through these applications.

vii. Remote worker security

One of the dangerous ways of exposing data to attacks is by forwarding them to home. This activity can turn all of the security measures in an institution into a completely useless process. Workers have the tendency to move a non-finished work to their devices and personal computers at home so that they could work on it later at home. This is quite risky because often personal computers and devices are less secured compared to the corporate ones. While business operations become more and more dispersed and online, mobile workers increase the potential threat for data. One of the IT professionals indicated that improper handling of data such as moving files from an office device to a home computer that does not have proper IT security measures attracts information theft.

viii. Insider threat

Sometimes the problem is not that users ignore security threat but the users are the threats themselves. One of the IT experts interviewed asserted that when workers are discontented with

their jobs, peeved with their boss, or sentimental for any reason, they can become insider threats who can purposely damage or leak data.

ix. Database misconfiguration

During the SQL injection attack an sql query was injected into the system which was able to communicate with it. This normally arises when the database is not configured properly especially when validating user-supplied data and construction of SQL statements such that usersupplied data cannot influence the logic of the statement.

x. Lack of mechanism to lock users after several login attempts

The system seems to have a weak lock out mechanism or none at all. This was apparent during the experiment when several passwords were gathered through brute force attack. A measure such as blocking a user after several attempts can be used to allay brute force password guessing attacks. In such measures, accounts are usually blocked after three to five unsuccessful login attempts and can only be unblocked after a given period of time, through an unlock system, or intercession by an administrator. Account lockout systems should offer a balance between protecting accounts from illegal access and guarding users from being denied authorized access.

5.3 Human Factor Models of Security Vulnerability

The focus here is to design models to better understand the human factors as a link between attacker and technological components of an information system. This will help to shape policies towards protecting sensitive information and the systems in general. The models were designed according to human oriented criteria and not technological ones.

5.3.1 A model linking the human factor

Regardless of the technical measures put in place, information systems can be vulnerable to attacks if systems users are not incorporated in the security framework. Figure 17 shows the connection

of all the essential components on an Information Technology system under attack and where the human factor comes in.

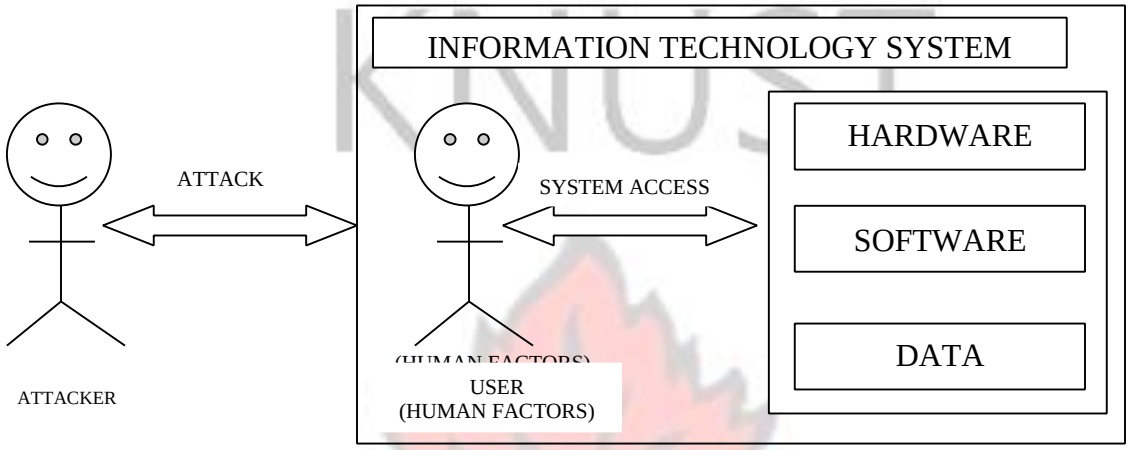

Figure 17: Linking the human factor

As indicated above, system users including their interaction with computers are the greatest loophole in Information Systems security. Information systems can be vulnerable to attack even if the best technical security measures such as firewall, IDS and antivirus are in place. The reason is that information security is not limited to the technological facet but must include the system users. Organization must therefore include system users when designing policies for data security.

5.3.2 Information security Vulnerability model

The aim of the vulnerability model is to highlight information system security vulnerabilities with particular emphasis on the human factors that were noted from the respondents.

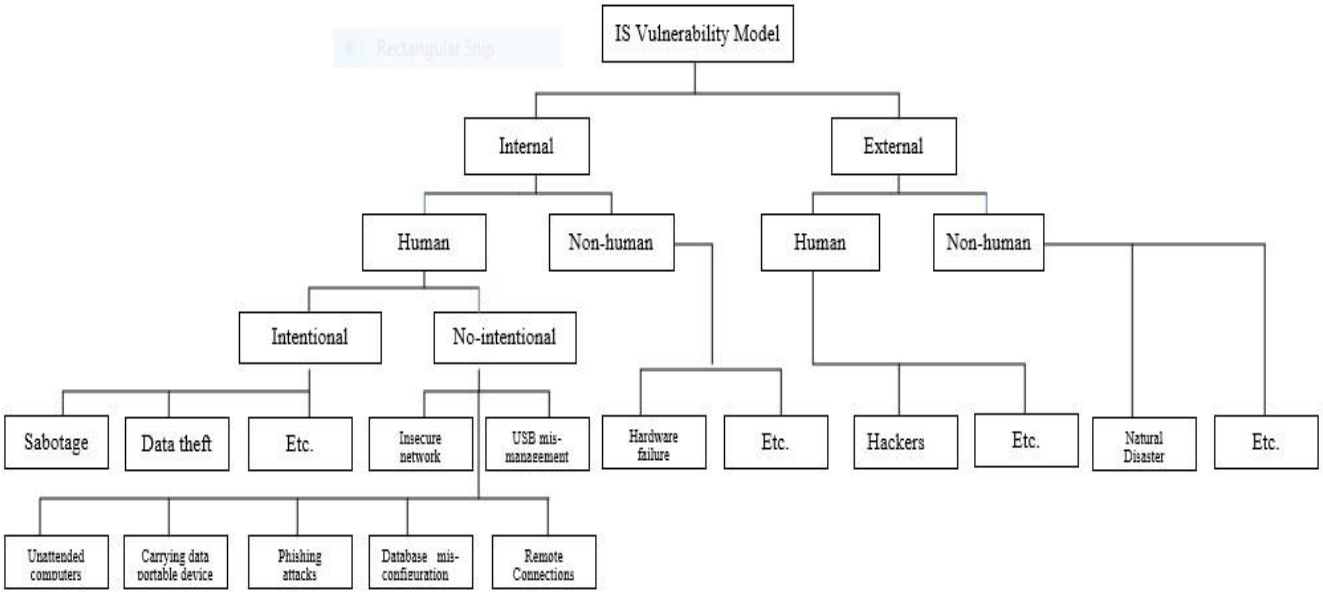

Figure 18: Information Security Vulnerability Model

5.4 Conclusions

The study has revealed that despite the fact that technology is important in the information security framework, technology alone was not enough to keep an organization secure from data breaches. Humans needed to be factored in to make the security framework holistic. It is not enough to say that the role of people is to run the applications. People can either be the weakest or the strongest link in the security framework and therefore should compensate for the deficiencies in the available security technology.. Therefore, there is the need to bring IT and human security together under a true information security management system. The increasing reliance on technological components of information security, makes securing information system increasingly challenging. Quite a number of the security problems emanate from humans because humans have the tendency to show their unethical attitudes when using information systems. Humans are therefore critical part that, when ignored, could affect information security efficiency.

Improving security using technical means is important for organizations conducting business online as well as for organizations that are at the same time seeking to realize their missions and goals. However, implementing technical measures does not guarantee a more secure environment. All sorts of human factors can severely affect the management of security in personal and organizational setting. Therefore, security is not exclusively a technical or technological problem; rather, people and organizations need to understand human factors, which need ample consideration in order to attain an effective information security management system practice.

5.5 Recommendations

Based on the findings of the study, it is recommended that for the human factor in information security to be managed effectively, the following should be taken into consideration.

a) Security awareness: Security consciousness and education are some of the most successful measures to mitigate the human factor threats to information security. In that regard, any information security plan should include a needs assessment that entails collecting information on the existing processes, the knowledge that is required of workers, and the cracks in the current information security.

b) Endpoint Security: Quite a number of information in institutions is not centralized.

Where there are centralized systems, information is often shared among workers and copied to different devices. Endpoint security is the notion that each device in an organization needs to be secured. It is recommended that sensitive information on portable devices like laptops and tablets should be encrypted. In addition, removable storage such as DVD drives and USB ports may be blocked if they are considered to be a major threat path for malware infections or data leakage. To secure endpoints, one needs extensive planning like applying policies that state that only certain computers like laptops can

connect to particular networks. Usage of wireless (WiFi) access points should also be restricted.

c) Recommended practices for working with portable and smart devices:

- Devices should be chosen carefully: All device have different security levels. For instance, iPads are built for general consumers and not as concerned by security and is therefore less innately secure than a BlackBerry device designed for business users.
- Turn on encryption: Once a device with stronger security controls has been chosen, the controls must be used.
- Require Authentication: it is essential that employees be required to turn authentication features on their devices so that lost devices cannot be easily broken into.
- Utilize Remote Wipe Capabilities: Employees should give IT administrators the capacity to remotely access and disable their devices in the event of loss or theft. This could be very handy in a situation where, say, an employee loses his or her device with sensitive data stored within.
- Third-Party Apps should be controlled: Smart devices are basically small computing devices that can accept any third-party applications and are therefore risky. It is recommended that unknown third-party applications should be limited to prevent people from seizing control of the devices.
- Set Unique Firewall Policies: people should set up unique firewall policies specifically for traffic coming from smart and portable devices. Smart device users don't necessarily need access to every bit of data on the network, so it makes sense to

limit exposure by only offering access to the types of data they need.

- Disable Bluetooth when not in use: Bluetooth capabilities on smart devices which can make it possible to talk on a hands-free headset can also be target for hackers who can utilise its 'always-on, always discoverable' default settings to launch attacks. In order to limit exposure, it is recommended that users deactivate bluetooth when it is not actively transmitting information.

d) A strong password should be enforced: it is recommended that functionality that rejects users from registering passwords that do not meet certain conditions should be used to ensure that only strong passwords are registered. A strong password should therefore have the following qualities:

- Be at least 13 characters in length
- Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)
- Have at least one numerical character (e.g. 0-9)
- Have at least one special character (e.g. ~!@#$%^&*()_-+=) Employees should also:
    - Not share their password with anyone at the work place
    - Change their password periodically o Password should not be written down or stored in an insecure manner o Reusing of password should be avoided o Usage of the same password for multiple accounts should also be discouraged.

- Organizations should use "timeouts" for all PCs to ensure that users are automatically logged out or that PCs are locked, to minimize the risk of insider attacks.
- Organizations should incorporate information security policies in their standard codes for conducting business. These policies need to be understood and implemented. workers must

realize that they play a critical role in maintaining corporate security and are responsible and accountable for security breach. Quality and security assurance should not be sacrificed for anything. Each worker should:

- Refer to the company's code, mainly those relating to information security, on daily basis to conduct business.
- In every business transaction they make they must be conscientious about security be it in the office or at home.

e) For information security threats to be curbed, organizations must adopt a holistic security framework, incorporating the human factor vulnerability to it. Based on the findings of the research, it is recommended that the following security framework should be adopted:

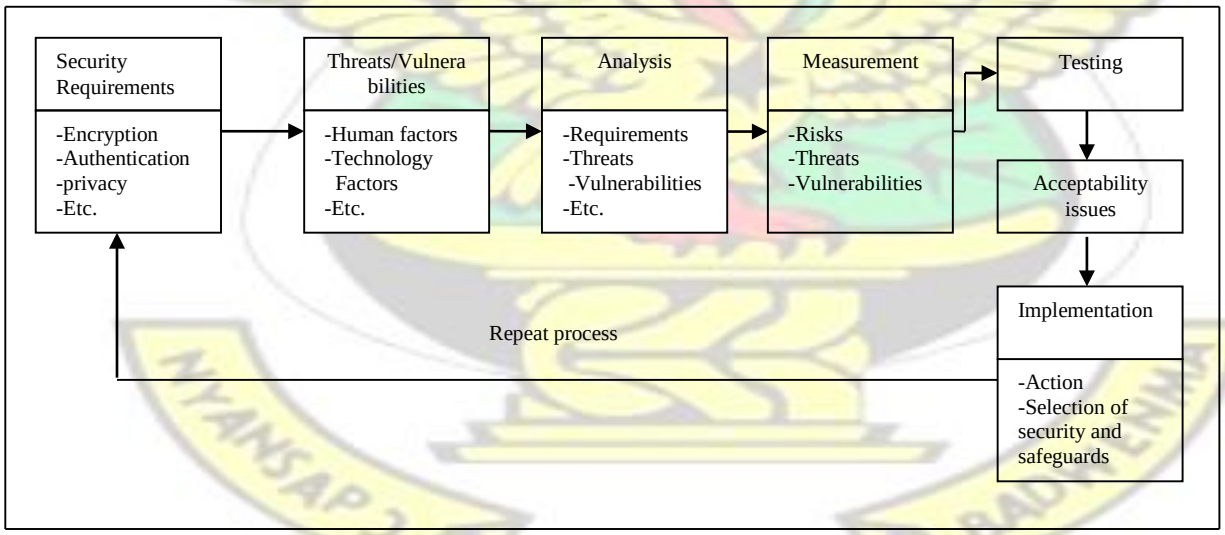

Figure 19: A holistic framework for information security

BIBLIOGRAPHY

Alhazmi, H. O. (2005). Quantitative vulnerability assessment of systems software. Annual Proceedings of Reliability and Maintainability Symposium (pp. 615 -620). IEEE

Anita, G., Kavita, K. and Kirandeep, K. (2013) Vulnerability assessment and penetration testing. *International Journal of Engineering Trends and Technology* 4 (13).

Beizer, B. (1990). Software Testing Technique (2nd Edition ed.). New York, USA: Van Nostrand Reinhold Co.

Bogdanov, A., Khovratovich, D., and Rechbereger, C. (2011) Biclique Cryptanalysis of the full AES. http://research.microsoft.com/en-us/projects/cryptanalysis/aesbc.pdf

Chan, M., Woon, I., and Kankanhalli, A. (2005) Perception of information security at the work place: Linking information security climate to compliant behavior. *Journal of Information Privacy and Security, 1(3),* 18-41.

Cisco (2006) "Understanding Remote Worker Security: A Survey of User Awareness vs. Behavior,"(http://www.cisco.com/web/CA/pdf/Understanding_Remote_Worker_Security_

A_survery_of_User_Awareness_vs_Behaviour.pdf), (accessed 2013 September 5)

Credant Technology suyveys (2008). "Credant survey finds shoppers leave more than 5,000 Mobile Devices at Largest U.S. Shopping Malls" (http://www.globalsecuritymag.com/Credant-Technologies-Almost-60 000,20080916,5003.html), (accessed January 25 2013)

Elbaz, L. and Bar-El, H. (2000). Strength assessment of encryption algorithms. Tokyo: Discretix Technologies Ltd.

Eric, M. (2004). Fundamentals of Network Security. Sydney: McGraw-Hill Technology Education.

Eugene, S. (2005). The human factor in security. *Computers & Security*, 24 pp. 425–426.

Global threat Report, December 2011.

Honeywell's Industrial IT solutions (2012) Amerchem cyber security vulnerability assessment

Howard, M., LeBlanc, D., & Viega, J. (2010). 24 Deadly Sins of Software Security- Programming Flaws and How to Fix Them. McGraw-Hill

James, A. K., Barton P. M., Eduardo, C. and Elisa, H. (2009) "First principles vulnerability assessment," (http://research.cs.wisc.edu/mist/VA.pdf), (accessed 2014 February 21)

Kamara, S., Fahmy, S., Schultz, E., Kerschbaum, F., and Frantzen M. (2010) "Analysis of vulnerabilities in internet firewalls," (https://www.cs.purdue.edu/homes/fahmy/papers/firewall-analysis.pdf), (accessed 2014 March).

Kashefi, I., Kassiri, M., and Shahidinijad, A. (2013) A survey of on security issues in firewall: a new approach for classifying fire wall vulnerabilieties. *Internationla Journal of Engineering Researh and Applications (IJERA)* 3 (2). pp. 585-591

Kaspersky Lab. (2013). "Software vulnerabilities," (http://www.securelist.com/en/threats/vulnerabilities?chapter=35), (accessed on June 20, 2014)

Kaye, K. (2002) Vulnerability assessment of a university computing environment. Swansea :SANS Institute:

Kruger, H.A. and Kearney, W.D. (2006). A prototype for assessing information security awareness. *Computers and Security, 25*, 289-296

Krsul, I. V. (1998). Software Vulnerability Analysis. Phd Thesis, Purdue University

Lamar, A. (2012) "Types of threats to database security," (http://www.brighthub.com/computing/smb-security/articles/61402.aspx), (accessed 2014 March 18)

Lesia, L. C and McCauley-Bell, P. R (2007). The human factors issues in information security: What are they and do they matter? *In Proceedings of the Human Factors and Ergonomics Society*, pages 439–443.

Matsui, M. (1994) Linear cryptanalysis method or DES cipher. *Advances in CryptologyEUROCRYPT '93*, pp 386-397

Microsoft Security Intelligence Report Volume 11, January-June 2011.

Mitnick, K.D. and Simon, W.L. (2002). The Art of Deception: Controlling the Human Element, Indianapolis: Wiley Publishing Inc.

Moore, H. D. (2007). Exploiting Vulnerabilities. Presentation Slide, Secure Application Development (Secappdev.org)

OWASP Organization. (2013). "The Open Web Applications Security Project," (https://www.owasp.org/index.php/Category), (accessed on April 3, 2014)

Philip S. A., Robert H. A., Richard M., and Michael S. (2003)The vulnerability assessment and mitigation methodology. Santa Monica: RAND.

Schneier, B. (2000). Secrets and Lies, Illinois: John Wiley & Sons.

Shulman, A. (2006). Top ten database security threats. Foster City, CA: Imperva Inc.

Soomro, A. W., Nizamudin, A., Iqbal, U. and Noorul, A. (2013). Secured symmetric key cryptographic algorithm for small amount of data. *3rd International Conference on Computer and Emerging Technologies (ICCET).*

Silver, P. (2013) Vulnerability assessment with application security. WA : F5 Networks, Inc.

Smith, R. D. (2004) Public servers vulnerability assessment report. Swansea: SANS Institute

The billion dollar lost laptop problem. Intel, Ponemon Institute 2009.

Vipindeep, V., & Jalote, P. (2005). List of Common Bugs and Programming Practices to avoid them. Technical Report, Indian Institute of Technology, Kanpur.

Whitman, M., Mattord J. H. (2005). Principles of Information Security, Sydney: Thomson.

William, L. S. and Mitnik K. D.(2002). The Art of Deception, Indianapolis: Wiley Publishing Inc.

Wilson, A. (2006) Marketing research: an integrated approach. London: Pearson Education Inc.

Willy, J., Amel, M. and Ana, C. (2007) "Software Vulnerabilities, Prevention and Detection Methods: A Review", (http://www-lor.int-evry.fr/~anna/files/sec-mda09.pdf), (accessed 2014 February 21)

2005 FBI Computer Crime and Security Survey

APPENDIX A

Interview

1. What is data security?

   ……

   ……

2. What are some of the technologies used to protect data?

   ……

   ……

3. Are these technologies enough in protecting data?

   ……

   ……

4. Do you consider human beings as part of the security framework?

……

……

5. What are some of the human actions that can make data vulnerable or at risk of attacks?

……

……

6. Do you have any recommendations that can curb the human actions which expose data?

.....

……

APPENDIX B

Survey

(Google form was used to conduct the survey)

Please tick as appropriate

Level

- 100
- 200
- 300
- 400
- Staff

Have you ever responded to an online request to provide your account or profile details?

- Yes
- No

Has your work or home computer ever been infected by malicious software? (e.g. virus, spyware)

- Yes
- No

Which of the following do you use for generating password? Check all boxes that apply.

- Personal information (e.g. data of birth, place of birth, address, name)
- Phrases
- Numbers
- Symbols
- Lowercase letters
- Uppercase letters
- Combination of the above

- ☐ Other: _____

On average, how long in characters are your generated password?

- ☐ up to 7 characters
- ☐ 8 or more characters
- ☐ As short as the system accepts

On average, how often do you change your password?

- ☐ At least once every 3 months
- ☐ At least

- ☐ once every 6 months
- ☐ At least once every year
- ☐ Only when required by the system
- ☐ Never

Do you reuse the same password for several user accounts?

- ☐ Yes
- ☐ No

If your password is difficult to remember, would you write it down?

- ☐ Yes
- ☐ No
- ☐ May be

- ☐

Do you prevent others from watching you type when you enter your username and password?

- ☐ Yes
- ☐ No
- ☐ Yes

Would you open an email link or attachment from an email address you do not recognize?

- Yes
- ☐ No

Would you share your username and password with someone else? (e.g. friend, spouse, colleague)

- ☐ Yes
- ☐ No

Would you enter your username and password on a website whose address does not start with "https://"?

- ☐ Yes
- ☐ No

You received a message which is labeled as "critical security updates and installation instructions", would you install it?

- ☐ Yes
- ☐ No
- ☐ Yes
- ☐ No
- ☐ I don't know

○

When attending to other matters do you log off your computer? 1. When leaving work premises?

○ Yes ○ No

2. When attending to a meeting?

○ Yes ○ No

3. When using the wash room?

Yes

○ No

4. When closing from work?

○ Yes ○ No

Powered by
Google Forms