

A STUDY ON EMPLOYEE INFORMATION SECURITY: HUMAN ISSUE:
GABORONE UNIVERSITY COLLEGE OF LAW AND PROFESSIONAL
STUDIES (GUC)

AUTHOR: THIMBONDE HAINGURA

STUDENT ID: 1818264

MSc IN COMPUTER SYSTEM MANAGEMENT

BOTHO UNIVERSITY

SUBMITTED TO

FACULTY OF COMPUTING: DEPARTMENT OF NETWORK AND
INFRASTRUCTURE MANAGEMENT

SUPERVISOR D.R SRINATH DOSS

ACADEMIC YEAR: JULY 2019

TABLE OF CONTENTS

List of tables.....	i
List of Figures	ii
Acknowledgement	iii
Declaration	iv
List of Abbreviation.....	v
Abstract	1
CHAPTER 1	3
1.1 Introduction.....	3
1.2 Background study	4
1.3 Problem Statement.....	5
1.4 Aims of the study.....	6
1.5 Objectives of the study	6
1.5.1 Research questions	6
1.6 Significance of the research study	7
1.7 Scope of the study.....	7
CHAPTER 2	7
2.1 literature Review.....	7
2.2 Definition ISA and the Human factor	8
2.3 overview of Information Systems in organizations.....	8
2.4 Over view of Information and Information Security	9
2.5 Human Threats to Information Security	10
2.6. Impacts of malicious and none malicious employee on IS.....	12
2.6.1 A compromise on CIA triad.....	12
2.6.2 Attacks on Passwords.....	13
2.6.3 Attacks on Emails.....	15
2.7 Counter Measures to Insider Threat	16
2.7.1 Information Security Awareness (ISA).....	19
2.7.2 Information Security Awareness Tools and Approaches.....	21
2.7.2.1 ISA Tools	21
2.7.2.2 ISA Approaches.....	21
2.7.2.3 Designing ISA awareness program.....	23
2.8 Information security frame works	26

2.8.1 ISO/IEC Standards	26
2.9 Theoretical Research Models	29
2.9.1 Protection Motivation Theory (PMT)	29
2.9.2 Theory of Planned Behavior (TPB).....	30
2.9.3 Technology Acceptance Model (TAM)	32
CHAPTER 3	33
Research Design and Methodology	33
3.1 Quantitative	33
3.2 Sampling	33
3.3 Data collection	34
3.3.1 Secondary data:.....	34
3.3.2 Primary data	34
3.4 Data collection instruments	34
3.4.1 Questionnaire	34
3.5 Ethical considerations.....	35
CHAPTER 4 RESULTS	35
CHAPTER 5 DISCUSSION	41
CHAPTER 6 CONCLUSION	44
CHAPTER 7 RECOMMANDATIONS.....	44
LIST OF REFERENCE.....	48
APPENDIX	54

List of tables

1. Counter measures to information security	17
2. Participant's security controls.....	18
3. Population sampling	33
4. Participants' Age Characteristics.....	36
5. Participant's password length distribution.....	38
6. Participants responses on malicious software protection.....	40

List of Figures

1. Elements of Information System	9
2. Vulnerability of Human Factors.....	11
3. CIA Triad	12
4. Active Attack.....	13
5. Social Engineering attacks.....	16
6. human factors that can influence security controls.....	19
7. Password Management Apple's iCloud Keychain:.....	23
8. Password Management KeePass.....	23
9. Training needs assessment	24
10. Information risk elements	26
11. Elements of IRM.....	27
12. Incidents response by users.....	28
13. Theory of Planned Behavior.....	31
14. Gender distribution.....	36
15. Participants educational background.....	37
16. Participants field of study.....	37
17. Participants' response on password security.....	38
18. Participants knowledge on types of threats.....	39

Acknowledgement

I am very grateful working with my project supervisor Dr. Srinath Doss for the outstanding advice and encouraged the spirit of working independently on the dissertation. I also extend my profound gratitude to Botho University support staff for all the help they rendered prior and during preparation for the dissertation. I also would like to acknowledge my family for showing keen interest and provided an inspiring and supportive environment on my schoolwork. I also acknowledge my friends for their support and encouragement to complete the program.

Declaration



BOTHO UNIVERSITY

PROJECT/DISSERTATION DECLARATION FORM

Name:	THIMBONDE HAINGURA
Student ID:	1818264
Programme of Studies:	MSc in Computer System Management
Module Code/Name:	Dissertation/C9-PWD-15
Title of Project/Dissertation: AN INVESTIGATION THE LEVEL OF INFORMATION SECURITY AWARENESS AMONG END USERS: HUMAN VULNERABILITY	
Name of Supervisor(s): Dr. Srinath Doss	
Declaration: In accordance with the appropriate regulations, I hereby submit the above dissertation for examination and I declare that: (i) I have read and understood the sections on Plagiarism and Fabrication and Falsification of Results found in the University's "General Information to Students" Handbook (2017) and certify that the dissertation embodies the results of my own work. (ii) I have adhered to the 'Harvard system of referencing' for referencing, quotations and citations in my dissertation. Each contribution to, and quotation in my dissertation from the work of other people has been attributed, and has been cited and referenced. (iii) I have not allowed and will not allow, anyone to copy my work with the intention of passing it off as his or her own work. (iv) I am aware that I may have to forfeit the certificate/diploma/degree in the event that plagiarism has been detected after the award. (v) Notwithstanding the supervision provided to me by the Botho University, I warrant that any alleged act(s) of plagiarism during my stay as registered student of the Botho University is entirely my own responsibility and the Botho University and/or its employees shall under no circumstances whatsoever be under any liability of any kind in respect of the aforesaid act(s) of plagiarism.	
Signature:	
Date:	04/10/2019

List of Abbreviation

CIA: Confidentiality Integrity and Availability

ISA: Information Security Awareness

IS: Information Security

TPB: Theory of Planned Behavior

PMT: Protection Motivation Theory

NIST: National Institute of Standards and Technology

IT: Information and Technology

NIST: National Institute of Standard and Technology

ICT: Information Communication and Technology

ISACA: Information System Audit and Control Association

OECD: Organization for Economic Corporation and Development

PU: perceived Usefulness

POEU: Perceived ease of use

IRM: Information Risk Management

ISO/IEC: International Organization for Standardization and International Electronic
Technical Commission

Abstract

The purpose of the study was to establish the level Information Security among End User in order to address the Human issue and its impacts on Information Security (IS) in organizations. Human errors likely to result into excessive security breaches than technical vulnerabilities (Hinson, 2003). Notable human errors include, deleting wrong file by mistake, entering wrong value, pull out the wrong plug by mistake and configuration mistakes can leave the network ports open, firewall vulnerable and system completely unprotected (Hinson, 2003). Employee errors impact negatively on security controls such as firewalls and data protection policies adopted by the organization (Hadlington, 2018). Human issues are the major hindrance in achieving security goals such as maintaining confidentiality, insuring integrity, and assuring availability of information in an organization (Cherdentseva and Hilton 2013). It is also notable that employees who either work inside or outside the organization can compromise the essential characteristics of information such as Confidentiality, Integrity and Availability (CIA). Despite intense technical and physical security controls adopted by the organization, the availability of malicious and none malicious employee in an organization hinders the effectiveness of counter measures adopted to protect information (Greitzer and Hohimer, 2011). A none malicious employee is an employee who is not aware of security controls adopted by the organization and lack efficiency to protect data from threats but instead create security loopholes which can be exploited by an attacker. A malicious employee has the motive to disrupt, steal information, bypass processes and procedures. However, none technical security counter measures such as security awareness, training and organizational policy implementation can be used to mitigate internal threats (Cherdentseva and Hilton 2013). In order to understand the human issue information security, the research study adopted theoretical research models such as Protection Motivation Theory (PMT), Technology Acceptance Model (TAM) and Theory of Planned Behavior (TPB) Shenbagaraman 2016). The research population included Lecturers and Administrative personnel in the organization. The independent variable included employee behavior, attitude and knowledge which were measured against dependent variables such as password usage, email usage, knowledge on malicious protection and security controls in the organization. Quantitative research methodology was adopted because data collected was translated into figures for further analysis. A questionnaire of 33 questions were distributed to 32 participants to collect data. The survey found out that some employee engages in risk behavior such as sharing password, using the same password to log in different systems or applications. Some employee in the organization also lack knowledge on threat to information security and are not security conscious to online cyber scams.

Key words: Information Security, Information Systems, Awareness, Policy, Social Engineering, Human factor, Insider Threat, outsider threat

CHAPTER 1

1.1 Introduction

The Human issue is among the threat to information security faced by organizations as compared to environmental and technological threat (Greitzer and Hohimer, 2011). Human issue refers to threats arising from internal or external employees in an organization which can pose potential danger to information security and other assets (Safianu, Twum and Acguah 2016). It is worth noting that insider threats impact negatively on efforts to maintain confidentiality, insure integrity, and assuring availability of information in an organization (Cherdentseva and Hilton 2013). It is also well acknowledged that employee breach confidentiality of information when they access, copy and use information which they not been authorized (Sethi, Kaur and Kumar 2011). Certain behavior of employees also affects the Integrity of information since data can be intentional or unintentionally created, deleted without authorization. Information Integrity can also be violated when employees improperly shut down computers (Sethi, Kaur and Kumar 2011). In the absence of data integrity, information cannot be trusted and it can negatively impact on policies and processes leading to poor decision making by management. Universities use Information Systems to manage confidential information related to finances, employee data, student data, academic programs, trade secrets, important research, suppliers and data of affiliated institutions (Razek, Kandari and Alawi 2016). However, Organizations spend more money and effort on technical and physical security controls without paying attention to human issues that can affect the confidentiality, integrity and availability of information (Hadligton, 2018). (Safianu, Twum and Acguah 2016) has shown that, regardless of the number of security controls in place, organization will continue to experience security breaches. (Safianu, Twum and Acguah 2016) also noted that IS is not only a technical problem but also a human issue. Human issues implies to activities performed by employees which can compromise IS which can be linked to disgruntled employees, risk behavior, poor attitudes towards security controls, theft and lack of knowledge. It cannot be disputed that the adoption of other technical controls such as firewalls, intrusion detection system, Data Encryption Standard (DES) were introduced as a solution to ethical issues like hacking, viruses and software piracy (Ugbogbo and Michael 2016). Some remedial actions to this problem are that, employees must be aware of security controls in place so that they understand the basic utility of security controls required (Hadlington, 2018). (Hadligton, 2018) noted that employees are the weakest link with respect to cyber-attack operations. ISA is therefore a vital tool that can be used to improve the

protection of IS in an organization (Metalidou et al. 2014). Employee weakness gives attackers an opportunity to gain access to confidential information in the organization regardless of technical control implemented (Greitzer and Hohimer, 2011). (Steyn and Drevin2007) also studied that ISA can help mitigate employee negative behavior, erroneous actions, data theft and misappropriation of information. (Metalidou et al. 2014) added that ISA is a vital tool that can be used to mitigate the Human factor threat by raising the level of employee's understanding on security controls adopted by the organization. (Kranz and Haeussinger 2013) has shown that lack of IS in an organization can result into problems such as financial loss, compromise of intellectual property, suffer potential law suits, bad reputation and competitors can take advantage of the information to improve their services and products. (Veiga, 2015) studied that lack of ISA among employees could lead to behavior that could result in potential information security incidents and data breaches such as the use of external portable drive which are not safe for backup and saving trade secrets in an unprotected cloud environment. (Goutam, 2015) noted that information security practices like avoid sharing password and updating of antivirus helps employees mitigate risks associated to identity theft and virus attacks. The same assertion was made by (Hash and Wilson, 2003) who has shown that taking precautions to system updates and use of strong passwords helps mitigate the risks of exposing information systems to cyber-attacks. (Valiente, 2016) has also shown that building a culture of cyber compliance and awareness in an organization is the most cost effective way of mitigating malicious activities. (Metaledou et al, 2014) noted that ISA is a tool that can also be used to change attitude, knowledge and behavior of employees. Targeted -attacks greatly affects elements of information security such as CIA. As a result, lack of ISA among employees makes these types of attacks undetected due to lack of reporting on suspicious activities by employees who encounter with malicious activity when using computers.

1.2 Background study

It is very crucial to protect the essential elements of information such as Confidentiality, Integrity and Availability (CIA) (Whitman and Mattord, 2011). According to (Cengage Learning n.d) security is the state of an organization of being free from danger. IS entails the protection of Confidentiality, Integrity and Availability of information assets which could either be in storage, process or transmission. Information security is effectively attained through security policy, education, training and awareness (Cengage Learning n.d). The Human issue has a major contributing factor on failure by organizations to protect business services, information systems and information (Metalidou et al. 2014). Information security

cannot be achieved if employees in an organization have negative attitudes towards security policies and lack knowledge on existing threats to information security.

A study titled “Understanding cyber scams: an assessment of the challenges of law enforcement in Botswana” by Lesedi Mashumba (Mashumba, 2016) established an insight about the effects of cybercrime, Botswana’s experience in cyber scams. Furthermore, it recommends that raising awareness among employees, individuals and enacting laws will help combat cybercrime. However, no effort established to investigate the level of IS among employees in organizations.

Also a research study titled “Legislating against cybercrime in southern African Development Community: Balancing International Standards with Country Specific” by Lewis C. Bande (Bande, 2018) discusses on enacting domestic legislation to compact cybercrime and put more emphases on criminalizing some cyber behaviors. However, it does not focus on raising cyber security awareness among users as putting stiff penalties would not stop cyber criminals.

1.3 Problem Statement

The Human issue is a challenge faced by many organizations as technical controls can be bypassed by human intervention. The human issue is worsened by lack of knowledge on threats to information security among employees in organization which leads to a compromise of confidentiality, integrity and availability of information (Colwill, 2009). Security breaches can also arise from employee attitudes and behavior towards security controls put in place to protect data. Organizations invest a lot of money and resources on physical and technical security controls to protect data and other resources and do not pay attention to employee actions that can expose information and other organizational assets to cyber-attack (Metaledou et al, 2014). Weaknesses in employee is a vulnerability that can be exploited by an attacker through malicious acts such phishing attack (Khan et al, 2011). There has been limited survey on the human issue and its effect on security controls established to protect computers and information in organizations as a result the research study is conducted to close the gap. It also noted that previous research conducted on the Human Factor or issue were mainly on large reputable organization and less attention to emerging organization in Higher Institutions of Learning in Botswana. There has also been limited emphasis on awareness and training among End Users of Information Systems hence, compliance to security policy in organization remains a challenge which negatively impacts on the goals of IS. Therefore, the research study investigated the level of IS among End Users. (Valiente, 2016) has shown that ISA and training

is the most cost effective way of mitigating malicious and none malicious activities. The research study was also triggered by the following reports linked to the human issue.

90% of organizations are vulnerable to insider attacks (Schulze 2018)

Universities in Africa face an age of cybercrime (Sawahel, 2017).

The study took into consideration that, **End Users** as employees working in an organization and have authorized access to network resources through a user account on the server or have physical access to the organization premises. End users were the major focus in the research study.

1.4 Aims of the study

The aim of the study was to investigate employee ISA to address the Human factor threat in the organization.

1.5 Objectives of the study

The following objectives were defined in the research study

1. To understand the impact of End User knowledge, behavior and attitudes on information security.
2. To find out how End Users understand counter measure put in place to protect information security.
3. To investigate End User compliance to information security policy in the organization.
4. To investigate if End Users have been exposed to awareness programs
5. To understand the importance Information Security Awareness (ISA) in organization.
6. To establish if the organization is in accordance with ISO/IEC standards

1.5.1 Research questions

The research questions were aligned to the aims and the objectives in order to get answers to the problem and were set as follows

1. How End Users handle their login credentials?
2. How End Users react to unknown email links?
3. How End Users perceive malicious threats to information security?
4. What are the factors influencing End Users intentions to engage in risk behavior?
5. Do End Users comply with information security policy?
6. How End users understand Information Security Awareness measures?

7. How to develop policies in order to change the behavior, attitudes and knowledge employees?

1.6 Significance of the research study

The study will help organization to realize that ISA is an important tool that can be adopted to address the Human factor and add a layer of defense on physical and technical security controls. The study will help organization to consider refining data protection policy or establishing data protection policy such as, password management policy, email policy and adoption of other security frame works to secure information from insider and outsider threats. Organization will benefit from the study by coming up with ISA training program to change End User risk behavior. Employee will also benefit from the study as they will acquire knowledge on security and subsequently engage in the most secure behavior to protect CIA. The researcher will benefit from the study by gaining an understanding of the human factor in organizations and possible solutions. The study will also contribute in the research field of information security with respect to the human factor threat in organizations.

1.7 Scope of the study

The scope of the study included but not limited to investigation of employee Information Security Awareness at Gaborone University College of Law (GUC) in relation to information security controls adopted by the university and ISO/IEC frameworks. Human factor which was the focus of the research study included intentional and unintentional errors, lack of knowledge on threat to information security controls, employee cognitive skills linked to behavior and attitudes which can make information and system vulnerable to cyber-attacks (Badie and Lashkari, 2012). The research study was also centered around CIA Triad from different sources of information linked to the human factor. The researcher study also focused on incidents that a user encountered when using computers at work which has an internet connection. The study only investigated End Users such as Lecturer and Administrative personnel. The study excluded Information system personnel such as System Administrators and students in order to manage the scope. The study considered End Users as employee with authorized access to the network of an organization.

CHAPTER 2

2.1 literature Review

This chapter gives a theoretical insight of what other authors have written about the topic under investigation to support the theoretical research of the study. It includes a discussion of

different sources such as journals, conference papers, electronic databases, government publications and books.

2.2 Definition ISA and the Human factor

According (Khan et al. 2011) ISA is a way of insuring that employees in an organization have knowledge regarding rules and regulations established to protect information from internal and external threats. (Hash and Wilson, 2003) also articulated ISA focus on changing employee's behavior so that they can adopt good security practices to protect information in an organization. (Hash and Wilson, 2003) asserted that the significance of ISA is to enable employees concentrate on security measures. (Metalidou et al. 2014) defines ISA is the level of employee's understanding on the importance of information security, the individual security responsibility and take affirmative action's accordingly.

According to (Greitzer and Hohimer, 2011) the Human factor is the weakness of an organization's employees that can be exploited by cyber criminals particularly risk behavior, bad attitudes and lack of knowledge. (Karwowski and Glaspie, 2018) explained that the human factor refers to undesirable behavior of employees on information systems that can lead to security breaches such as disclosure of confidential information and unauthorized access to information.

2.3 overview of Information Systems in organizations

Information Systems is a combination of technologies such as computers, software's, communication links, mobile device used in organization and social context (Boell and Keemanovic, 2015). (Bhatnagar, Kumar & Gupta 2016) also articulated that Information systems are devices and software's used by end users to manipulate data and produce services. Employees use information systems to capture, store, retrieve and transmit information. Information systems faces a number of threats and vulnerabilities hence, employees must have knowledge and understanding of these emerging security threats (OECD, 2002). Information Systems are used to support business operations such as collecting, storing, creating, manipulating data (Rainer, Prince and Cegielski 2012). Figure 1 illustrate information system components.

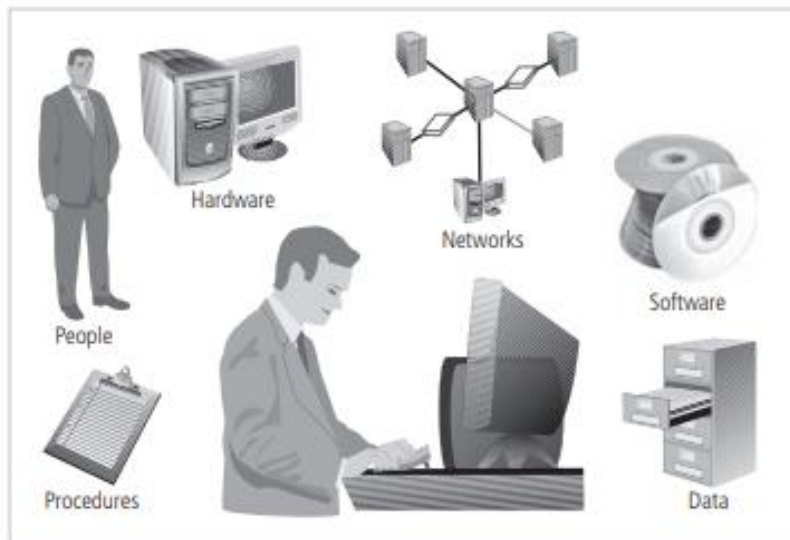


Figure 1 Elements of Information system: source (Cengage Learning n.d)

2.4 Over view of Information and Information Security

Information is an important asset of an organization which aid in decision making hence it must be accurate, reliable, complete, up to date and protected from internal and external attack (Maingak and Harsono 2018). (Whitman and Mattord 2011) noted that IS is the protection of essential elements of information such as Confidentiality, Integrity and Availability (CIA). IS is the establishment and implementation of security controls which could be technological, organizational, Human and administrative to insure that all information is free from threats (Cherdentseva and Hilton 2013). (Acguah, Twnm and Safiana 2016) studied that IS entails the protections of Confidentiality, Integrity and Availability. (Kranz and Haeussinger 2013) noted that lack of IS in an organization can result into financial loss, compromise of intellectual property such copy rights, trademarks and trade secrets, bad reputation and competitors can take advantage of the information to boost their services and products. (Whitman and Mattord, 2011) added that IS can be achieved through education, training and awareness. (Wawak 2010) also studied that information security is key to information confidentiality, availability and integrity. (Shareef 2016) also articulated that information security entails a process of eliminating issues that have the probability to cause damage or threaten security countermeasures put in place to protect information. According to (Fatt and Ping 2014) information security involves processes, technology and people elements. (Veiga, 2015) noted that information security incidents relate to any activity that can results in damage, corruption,

misuse or unauthorized exposure of confidential information. Employees related security incidents includes the use of external portable drive which is not safe for backup and saving trade secrets in an unprotected cloud environment.

2.5 Human Threats to Information Security

The major threat agents on information security and systems includes humans, natural disasters and technological agents. Threats can be internal, external or a combination of external and external entities. (Pfleeger, 2006) studied that threats to IS can be initiated by employees in an organization. Employee initiated threats are those threats that are related to incidents like errors, inexperience, improper training and irresponsible behavior on security controls among employees (Pfleeger, 2006). Internal threats take place when an employee who has been granted access to system resources and abuses the privileges. An internal threat can also result from employee action or failure of organizational process (Jouini, Rabai and Aissa 2014). External attackers can intrude information in many ways such as over the internet, physical invading the systems or through a private networks of affiliated business partners of the organization. Human threats encompass those threat caused by human actions like an insider which causes harm and disruption on information security or information systems. Computer initiated threats includes deliberate attack using malicious software's such as worms, Trojan horse, virus, logic bomb, backdoors and denial of service (DoS) attacks. Disgruntled employees with authorized access to Information Systems (IS) can inject Trojan horses to deliberately make IS vulnerable to attack (Jadhav and Yeshwantro 2014). Computer initiated threats are mostly perpetuated by an outsider and Human initiated threats are mostly perpetuated by insiders such as employees with privileges access to information. According to (Schulze, 2018) the most dangerous threats to information security are trusted employees. Employees actions can be classified as intentional malicious and unintentional or accidental malicious in an organization. Peculiar behavior of accidental actions which end up being malicious to information security is related to carelessness, negligence and compromising credentials by employees and peculiar behavior of deliberate or intentional malicious actions relates to willful causing harm or disruption to information security (Jouini, Rabai and Aissa 2014). (Choi, Levy and Hovac 2012) also noted that intentional insider abuse includes, risk behavior such as data manipulation, destruction and theft and also pointed out that unintentional insider abuse includes erroneous entry of data values which can compromise data integrity as well as poorly

trained and unmotivated users. Weakness of security best practices among employees in an organization enables an outsider exploits the weakness and launch key logger attack either through hardware or software installation. According (Badie and Lashkari, 2012) human factors such as “lack of awareness, user behavior, user belief, lack of motivation, inadequate staffing, inadequate use of computer security” also have negative implications on information security. Figure 2 illustrate the Human factors in an organization.

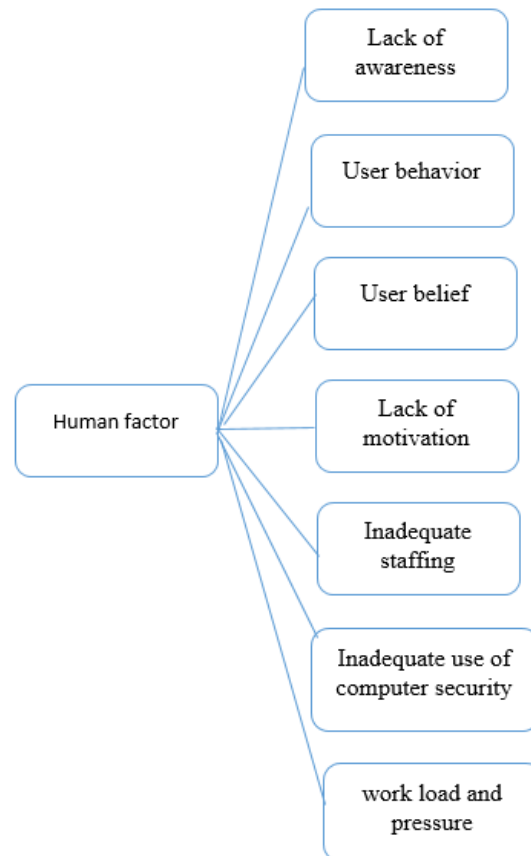


Figure 2 Vulnerability of Human Factors source (Badie and Lashkari, 2012)

Lack of awareness: Elements linking to lack of awareness among employees includes the following; users cannot able to recognize pattern or activity of malicious attack in the computer; they do not know the importance of creating a resilient password, they engage in activities that is prone to identity theft and social engineering attacks and users have difficult in controlling other employees in accessing each other’s computers (Metalidou et al, 2014).

User belief: human believe on particular security controls adopted by an organization is also associated to lack of knowledge. Some common believe among employees that have negative

impacts on information security are that, the installation of computer antivirus is not important as antivirus slower the processing speed of computers and users are always prepared to download or click on link from unknown source or insecure sites as they don't believe that such action would compromise information (Metalidou et al, 2014).

Lack of motivation: lack of motivation among employees can lead to lack confidence in adopting good secure behavior and best security practices. Employees can be motivated in an organization through awareness of security controls (Metalidou et al, 2014).

Inadequate use of computer security: if employees lack awareness on security basics such threats, risks and effects of none compliance on security policies, information security will not be effectively achieved in organizations. Some incidents that can result in un proper use of security controls encompasses actions such as unauthorized reconfiguration of systems, unauthorized access to security credentials like passwords of others and retrieving confidential information for self-gain (Metalidou et al, 2014).

2.6. Impacts of malicious and none malicious employee on IS

2.6.1 A compromise on CIA triad

The CIA triad is a guide for organizations to gauge their level of information security (Henderson 2017). Malicious employees within an organization can expose the Confidentiality, Integrity and Availability of Information (Colwill, 2009). (Quadri Suhail 2016) also emphasized that the CIA Triad is crucial guiding principle to information security policies in organizations. Figure 3 below illustrate the CIA triad

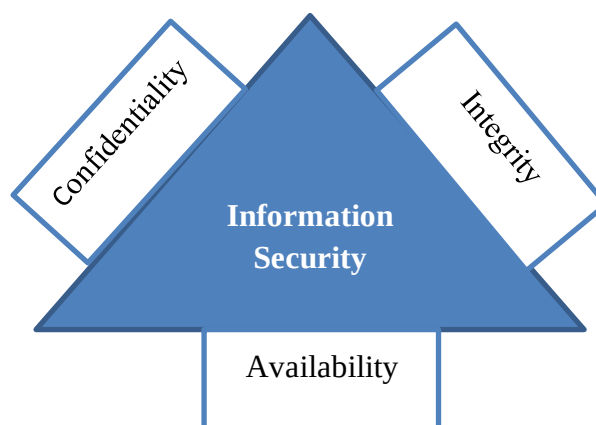


Figure 3 CIA Triad. Source (Cilliars, 2015)

Improper use of security controls by employees can result into creating security loop holes which can be exploited by Cyber criminals eventually interferes with CIA. (Pfleeeger, 2006) studied that attacks such as modification, interception, fabrication and interruption is a major threat on CIA. Inadequate use of computer security controls can give an opportunity to an outsider with malicious intent to exploit the system. If employees in an organization lack knowledge on the nature of social engineering attacks they can easily give away confidential information such as log in credentials and an attacker can use such information to launch an attack like interruption which greatly affects availability of services and information (Singh, Kumar 2011). If employees leave computers unattended, an intruder can gain access to unauthorized information into the systems and further engage an attack known as fabrication to encrypt files and legitimate users will not be able to authenticate into the system. Risk behavior like sending emails without encrypting the files can also compromise to the integrity of information (Hostiad and Surdama 2016). A typical Attacks on integrity is when a third party modify the contents of the message which eventually misled an employee decision making process. An attacker can disrupt communication between the sender and the receiver by taking advantage of human vulnerability. Figure 4 below depicts active attack modification

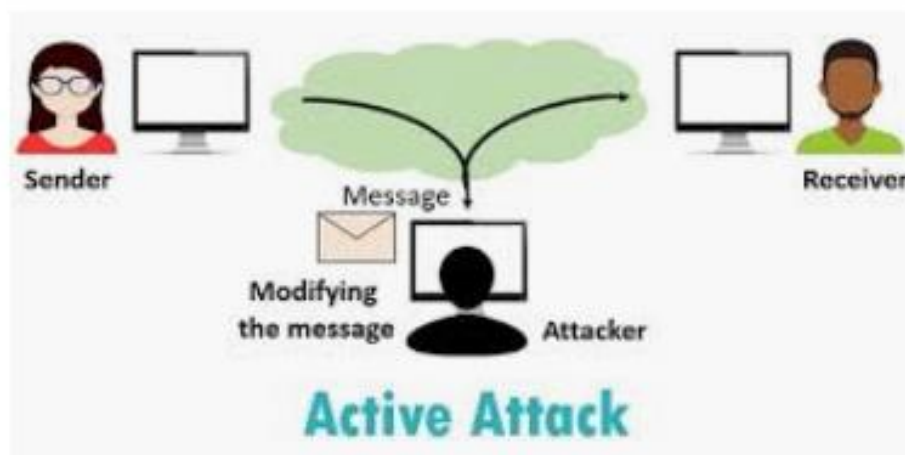


Figure 4 Active attack modification

2.6.2 Attacks on Passwords

According to (Kamal 2019) a password is a predominant means of authentication. A password is used to verify identity before a user gain access into the system (Blazevic, Ocevcic and Solic 2015). (Bartler, 2014) also asserted that a password is a first line of defense mechanism used by end users to protect information and systems from intruders hence poor handling of

password can compromise information security. Lack of security consciousness among employee like sharing of passwords enables disgruntled employee with malicious intent to have unauthorized access to organization network and cause harm or steal confidential information. (Singh, Kumar 2011) noted that an intruder can use a compromised password to carryout malicious activities. Passwords are used in the field of Information Communication and Technology (ICT) to log into various systems such as LinkedIn and Face Book, online banking accounts, Electronic learning like blackboard and portals, Automated Teller Machine (ATM), and electronic mail accounts (Kulkarni 2015). Hence using the same password to log into different application can compromise information security in case the password is compromised. (Kamal 2019) highlighted that password authentication mechanisms have many security challenges. There are some limitations of widely used hash functions like Message Digest 5 (MD 5) which can be exploited by an attacker. (Bartler, 2014) articulated that cyber criminals or hackers use different types of attacks to steal passwords stored in databases in a file format known as digest file (Kamal 2019). Hackers or cyber criminals can obtain user name and passwords stored in computers or device connected to the internet or get stored hash values and launch an attack like brute force and dictionary attack (Kamal 2019). If a Password is compromised, confidentiality and integrity is breached resulting in unauthorized users have access to private information in the organization. Attack on availability leads to sudden loss of connection and disruption to services like online transaction, sending an email or placing an order online. (Bartler, 2014) also studied that cyber criminals can crack legitimate user password using special tool like Rainbow crack and malicious software such as key logger to capture username and password without the user's knowledge. (Gao et. al, 2018) asserted that weak password can easily be guessed by attackers. (Kulkarni, 2015) outlined different methods of password attack as follows

Dictionary attacks. An attacker can generate thousands of candidate digest and create a huge lookup table with the generated digest and their predefined plain texts passwords. Hackers compares the generated digest file with stolen digest file and if the is a match, they retrieve the password.

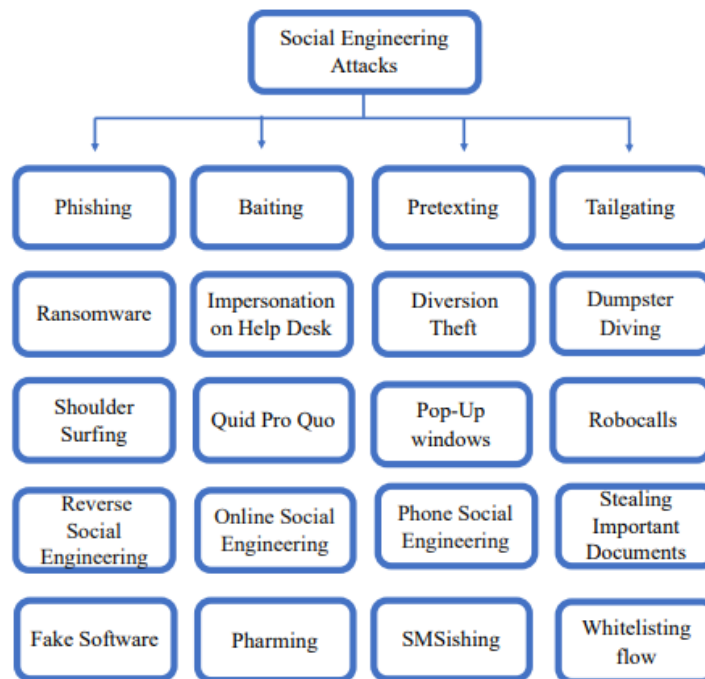
Brute Force attacks: an attacker can use computers software's as weapon to systematically cycle through each letter in the character set to guess the password. A character set can be special symbols, numbers, or anything of interest to an attacker and very helpful to accomplish the mission. The attacker tries a combination of passwords and this method of attack works best for shorter passwords. According to (Blazevic, Ocevcic and Solic 2015) it is important for

create strong passwords and avoid sharing password and writing down password on a piece of paper. (Blazevic, Ocevcic and Solic 2015) emphasized that three factor authentication is ideal. Best security practices like enforcing security awareness among end users can help lessen insecure behavior like sharing of password. Phishing and social engineering are commonly used by attackers to deceive users so that they can reveal their credentials or identity. (Blazevic, Ocevcic and Solic 2015) noted that there are plenty of tools that can help cyber criminals obtain user name and a password.

2.6.3 Attacks on Emails

According to (Solic, Nenadic and Galic 2012) unwanted mail message in the user inbox is a sign of malicious software. (Solic, Nenadic and Galic 2012) added that malicious attack could be spam, Trojans, and worms. (Solic, Nenadic and Galic 2012) emphasized that the riskiest ones are direct phishing attack targeting organizations. Phishing is a strategy used by attackers to manipulate individuals in order to steal confidential information (Sumari, Alomari and Rajalingam 2012). (Sumari, Alomari and Rajalingam 2012) also studied that cyber criminals design phishing emails and pop-up windows by incorporating official logos, web site design from real organizations and other information of interest that can be used to deceive end users. Cybercriminals use techniques such as Spear phishing, Phishing and Smishing to obtain information from innocent individuals. (Yadav Kumar and Chandel 2017) has shown that phishing is a technique in which cybercriminals sends unsolicited email messages to users claiming to be originating from famous organizations like banks, online shopping sites or the employee's employer site. Individuals are invited to click illegitimate link to update information related to Personal Identifiable Information (PII). (Yadav Kumar and Chandel 2017) also noted that cybercriminals use Smishing attack to target end users using mobile phones by sending Short Message Service (SMS) like "You have won yourself \$10000" and the SMS includes contact numbers. An attacker can also use Spear Phishing attack to send fraudulent emails to known individuals by enticing individuals using Facebook, LinkedIn to get specific information about individuals which can later be used to launch malicious attacks like installing key logger software such as Trojan horse to covertly collect confidential information. in order to mitigate this type of malicious acts, software tools like Key Scrambler, Spy shelter can be used by end users to prevent key logger phishing attack (Yadav Kumar and Chandel 2017). (Yadav Kumar and Chandel 2017) also noted that social engineering attack can be avoided by not sharing personal information to unknown sender or source unless the receiver

has verified the authenticity of the sender. (Kaabouch and Salahdine 2019) asserted that Social Engineering attacks are sophisticated and cannot be prevented using software's and hardware solutions but instead people needs to be educated on social engineering attacks. (Yadav Kumar and Chandel 2017) added that end users must always insure that the connection being used is secure to access the internet is secure. Figure 5 below illustrate types of Social Engineering



attacks.

Figure 5 Social Engineering attacks

2.7 Counter Measures to Insider Threat

Counter measure are the actions taken by an organization to counter threat or danger that can impacts negatively information security and Information Systems (Cherdentseva and Hilton 2013). An organization implements counter measure to achieve security goals such as integrity, availability, confidentiality, privacy, authenticity, trustworthiness, auditability and non-repudiation. Security counter measure includes, Technical, Physical and Administrative (Cherdentseva and Hilton 2013).

Table 1 Counter measures to information security: source (Cherdentseva and Hilton 2013)

Technical control	Administrative control Includes organizational policies and guidelines	Physical control:
--------------------------	--	--------------------------

Use of software and hardware				monitor and protecting physical environment
Authorization	Culture	Law	Procedure	Surveillance cameras
Authentication	Motivation	Contracts	Policy	locks
Cryptography	Education	Agreements	Governance	Access control: biometric access
Firewalls	Ethics		Strategy	Sensors for Heat, water, smoke
Intrusion Detection System	Training		Audit	

(Hinson, 2003) Contented that relying on technical controls does not satisfy the notion of layered defense to information security in an organization and articulated that awareness on existing technical, physical and administrative control is a cost effective form of security control as it adds another layer of defense. According (Rose, 2016) physical security is often ignored and its significance underestimated in favor of technical controls. (Battele 2015) noted disgruntled employee are a big threat to information security hence computer accounts and physical access for employee who left the organization should be suspended immediately. Active accounts not in use can also be an opportunity to trusted employee with malicious intentions (Battele 2015). Immediate reporting of active accounts not in use help avoid lope holes for malicious action (Battele 2015). Table 2 illustrate appropriate remedial actions to be taken.

Table 2 Employee security controls: source (Battele 2015)

✓	L/M/H	Activity / Security Control	Rationale
Choose an item.	L	Adequately screen candidates for hire and repeat the screening process at regular intervals for sensitive positions.	Provides a level of confidence that new hires are trustworthy and ensure ongoing trust in the employee.
Choose an item.	L	Include cyber security-related items in the employee termination and transfer process and/or checklist.	Ensures that access privileges are revoked at termination or transfer and that all equipment and data are returned to the facility, as applicable.
Choose an item.	L	Document misuse and abuse cases.	A written description of past problems should be consulted when designing protections to prevent future problems.
Choose an item.	M	Ensure that the employee evaluation process includes responsibilities related to cyber security, that these responsibilities are updated regularly, and they are managed to ensure they continue to address the facility's cyber security needs.	Ensures that job descriptions formally include cyber security responsibilities and that employee performance in this area is monitored and rewarded.
Choose an item.	M	Ensure that training and recruiting efforts are focused on cyber security.	Allows the facility to attract and retain top cyber security talent.
Choose an item.	M	Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor.	Accounts of contractors and employees who have been terminated can be misused to gain unauthorized system access. Disabling instead of deleting accounts allows preservation of audit trails.

Awareness on encryption technique can help employees understand and appreciate the importance of using Pretty Good Privacy (PGP) CIA of information (Hostiad and Surdama 2016). PGP can be installed on computers used by its employees in an organization. employees

can generate their own PGP key that can be used to encrypt email message and attachments before sending within or outside the organization.

Intrusion Detection System (IDS): human factors such as attention, vigilance, mental workload, situation awareness and multitasking can influence the capability of IDS (Sommestad nd). It is important for a user to response to alerts that has been set to detect the nature of the treats. However, user responses to system alerts can be affected by selective attention and divided attention (Sommestad nd). Selective attention is when a user selects and process the wrong information and divided attention is when a user focus on multiple tasks but struggle to handle them efficiently. The user must also be vigilance so that they can detect signal that are rare, unexpected and often of low to be noticed. Figure 6 illustrate human factors that influence IDS capability.

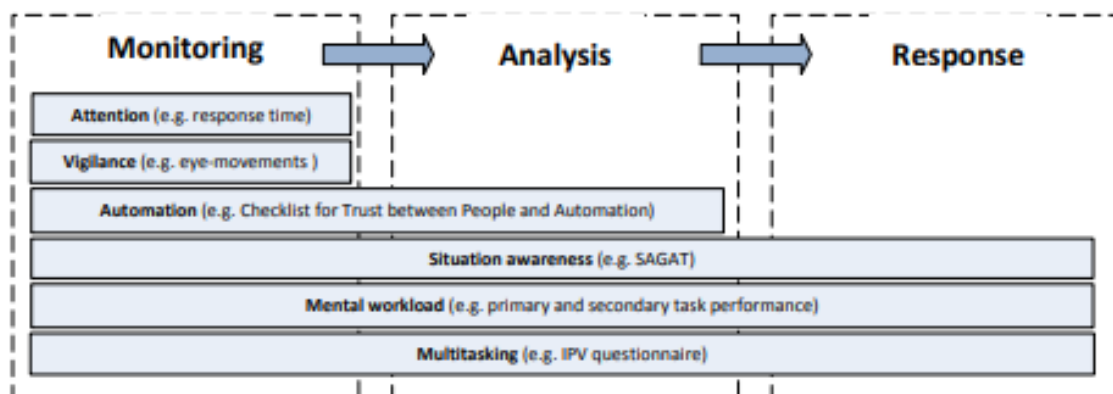


Figure 6 human factors that can influence IDS source: (Sommestad nd)

2.7.1 Information Security Awareness (ISA)

ISA is a useful tool that can be used to counter the Human factor threat since it is well acknowledged that employees can intentionally or unintentionally compromise information system in an organization. An insider is an employee with privileged access to Information System and misuses the privileges for personal gain (Probst and Hunker n.d.). ISA among employees can help address the human factor in information security (Greitzer and Hohimer, 2011). (Acguah, Twnm and Safiana 2016) has shown that deployment of technical controls, physical controls and forcing employees to sign security policy is not the ultimate solution to prevent insider threats. Due to the changing business landscape, business partners, temporary employees and consultants can have privileged access and as a result, they can be classified as part of an insider (Probst and Hunker n.d). Implementation of security controls and policy

must be coupled with ISA and training among employees who are hands on information systems (Acguah, Twnm and Safiana 2016). Lack of ISA among employees could lead to behavior that could result in potential information security incidents and data breaches (Veiga, 2015). Cases of security incidents are that employee can use external portable drive which are not safe for backup and saving trade secrets in an unprotected cloud environment (Veiga, 2015). (Khan et al. 2011) has shown that, effective security awareness can have positive impacts on information security. (Fatt and Ping 2014) studied that the aspect of technology focus on the use of hardware and software such as firewalls, encryption algorithm and penetration testing tools and argued that the importance information security is hindered by lack knowledge about security controls among computer users. (Acguah, Twnm and Safiana, 2016) noted that the use of hardware's and software's does not guarantee complete security of information in an organization and argued that employees must be involved to take part in protecting information through awareness. Technical solutions to information security can be best achieved if users have knowledge on how use the technical solutions in place effectively (Kaur, 2016). According to (Amarachi, Okolie and Ajaegbu, 2013) IS cannot be achieved effectively in an organization employees are lack awareness on the risks and threats to IS. The current information age requires attention to ISA (Norman and Yasin2010). According to (Kaur 2016) positive attitudes and commitment of users towards security controls helps secure Information Systems. (Kaur 2016) added that human and technology should be integrated to maximize security consciousness on security controls since human beings are the weakest link. (Metalido et al, 2014) pointed out that raising security awareness among individuals helps reduce risk behavior and the level of security breaches caused by human error. According to (Metalido et al, 2014) employees can prevent malicious activity if they are aware of existing threats in the cyber space. Users with lack of information security awareness cannot easily identify signs of malicious activity in their computers and realize the importance of using strong password by combining symbols, characters and numbers. (Chan and Mubarak, 2012) pointed out that there is an association between ISA and preventative action which can enhance security performance in organizations. According (Chan and Mubarak, 2012) security awareness can help instill knowledge regarding information security threats which can help employees protect information in an organization. Managing, mitigating risks and threats requires a concerted effort among all employees in order to understand how technological elements interplay so that employees can better relate factors that can lead to information vulnerability in an organization and how they can be mitigated (Werlinger, Hawkey and Beznosov, 2008). Information security is a human issue hence it cannot be attained effectively

through hardware's, software's and as requires that end users need to be equipped with knowledge and skills on how to handle security controls (Beyer and Brummel 2015). (Valiente, 2016) has also shown that cyber compliance and awareness is the most cost effective way of mitigating malicious activities. Human vulnerability is widely exploited by cyber criminals in the digital space as they use advanced hacking methods and tools to steal sensitive information (Aloul, 2012). (Denev and Hu 2007) asserted that in order to prevent and mitigates threats, it is not safe to depend on protective technologies like the use of intrusion detection systems, firewalls without involving employees. (Denev and Hu 2007) noted that human errors are threats to Information Security. (Denev and Hu 2007) also studied that information security is a socio technological problem hence it is significant to comprehend human behavior, knowledge, attitudes and their effects on protective technologies like firewalls. In other cases, end users have different perception with regard to protective technologies as other prefer to disable software security protection like antivirus with a perception that they slow the processing capability of computers. Human errors can severely lead to security breaches of intimate information such as usernames and password. In other cases, (Hadligton, 2018) has found out that employees are susceptible to social engineering attacks because there has been limited attention on the Human factor issue in the workplace. (Aloul, 2012) asserted that human vulnerability is also on the rise and it highly being exploited by cyber criminals. Cyber security practices are considered as an important part of individuals and families (Goutam, 2015). (Valiente, 2016) has also shown that building a culture of cyber compliance and awareness is the most cost effective way of mitigating malicious activities. Lack of knowledge on cyber security threats has potential to increase organizational susceptibility to cyber threats that can emanate from End users and eventually compromise information systems.

2.7.2 Information Security Awareness Tools and Approaches

2.7.2.1 ISA Tools

(Khan et al. 2011) noted that Information awareness tools entails the use of electronic mail messaging, group discussion, newsletter articles, computer aided training and posters.

2.7.2.2 ISA Approaches

(Hash and Wilson, 2003) has shown that educating employees on the following can help mitigate social engineering attacks.

Use of strong password: an effective password helps to counter attacks dictionary attacks which is a common threat to password security.

Backup data: data backup is a process of copying the original file and store it in a different logical or physical location. loss of data can happen either by accidental deletion of files, virus attack, software and hardware failures. Employees can back up word files, spread sheet files and data bases on external disk drive, USB Drive and compact disk and DVDs.

Use of updated antivirus: antivirus is a security tool that can help employees scan for malicious codes that could corrupt personal files and crash the systems. If the system crashes due to malicious attack, employees would not be able to access services which affects the element of availability.

Reporting suspected incidents of malicious activities: reporting incidents of malicious acts is a good security practice which helps prevent further occurrence of an attack. Malicious acts could be a stranger entering in an unauthorized office, risk behavior of some employees such as attempting to access an authorized information and disclosure of information to third party.

Effects of none compliance on security policy: employees must be aware that failure to comply with security policy is putting the organization and their job security at risks.

(Hash and Wilson, 2003) asserted that topics such as password usage or management, malicious protection, policy implications of non-compliance, email attachments, physical access, spam and social engineering attacks can be effective on sensitizing employees in an organization. Educating employees on ISA security policies can significantly improve employee's knowledge on computer related security, compliance and procedures (Karwowski and Glaspie, 2018). (Solic, Nenadic and Galic 2012) asserted that security awareness on password handling can help users change their behavior and adopt secure ways of keeping their password. (Solic, Nenadic and Galic 2012) also asserted that awareness helps user realize the importance of systems logout after use and updating antivirus software's. (Blazevic, Ocevcić and Solic 2015) added that password can be stored safely and be remembered using management tools such as KeePass and Apple's iCloud Keychain. Figure 7 below illustrates Apple's iCloud Keychain interface and figure 8 illustrates KeePass Interface.

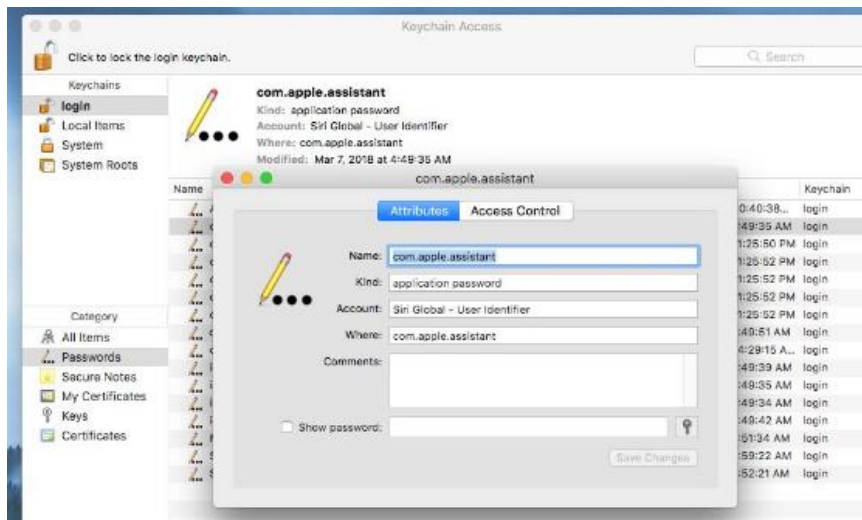


Figure 7 Password Management Apple's iCloud Keychain

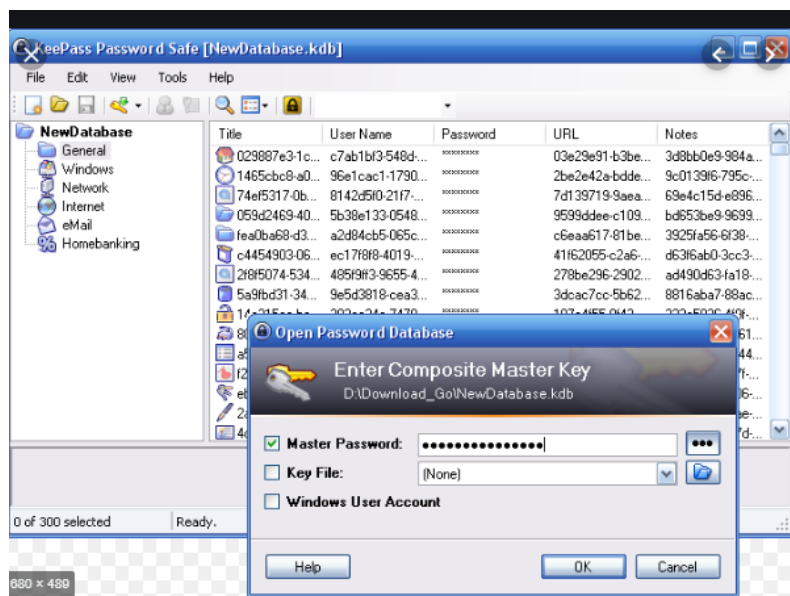


Figure 8 Password Management KeePass

2.7.2.3 Designing ISA awareness program

Awareness program can be used to deter malicious and non-malicious employee in an organization to close some internal security threat such as lack of security consciousness among employees (Hash and Wilson, 2003). A working Awareness program must be relevant to the information security problems experienced by the organization. (Hash and Wilson, 2003) has shown that there are 3 models that can be adopted in order to design, develop and implement an awareness program which includes; 1. Centralized Policy, Strategy and Implementation, 2.

Centralized Policy, Strategy and Distributed Implementation and 3. Centralized Policy, Distributed Strategy and Implementation

After identifying a suitable model for the awareness program, a need assessment must be conducted in order to establish areas of security controls that requires user awareness in an organization. However, (Hash and Wilson, 2003) noted that employees in managerial positions and system administrator and must take proactive actions to achieve security goals. (Hash and Wilson, 2003) emphasized that managers and users requires high level of security awareness and training on security controls. In order to maintain focus during the need assessment process assessment techniques like Interviews, Questionnaire and analysis on acts of malicious activities can be used. It is very crucial to understand specific issues as illustrated in figure 9 prior to the need assessment.



Figure 9 Training needs assessment. Source (Hash and Wilson, 2003) NIST Special Publication 800-50

Assessment of the information obtained: The assessment process should provide answers to key questions like what is needed in the awareness program, what ongoing activities being carried out to meet the needs, how effective in terms of addressing the needs, what else need to be done and which needs are most important. After a success full needs assessment follows the development of awareness, training strategy and plan (Hash and Wilson, 2003). The plan should include among others, scope of awareness program, target audience and topic to be covered in each session. After security awareness, training strategy has been completed, an implementation schedule must be put in place. However, some decision can be reached whether the implementation can be carried out in phases and in such cases following factors can be considered; availability of resources, state of recent compliance and critical dependency.

Awareness can be targeted on employees depending on the behavior identified (Hash and Wilson, 2003).

Continuous checks on employees

It is important that an organization should check the background on individual and they should be thoroughly screened to validate their previous employment through vetting before an individual is employed in the organization. Employee vetting help to establish traces of employees linked to behavior, attitudes with previous employment. However, monitoring of employees should be a continuously process as different circumstances can make employee change their behavior.

Data security program should be crafted around motivation, attitudes and behavior of employees in order to build human firewall (Lawroom report nd): such approaches includes the following

Cultivate a data security mind set: training should be aligned to employee attitudes and believes so that they think and beliefs. They must be empowered to take concrete actions to prevent security breaches in an organization.

Tell compelling stories: Employees can change the behavior if they listen to well-constructed stories on cyber scams and mistakes that employees did which compromised company information reflecting real life situations (Lawroom report nd).

Provide immersive interactions: employees should be given the opportunity relevant to the nature of attacks through simulations so that they can apply their knowledge and skills in realistic situations.

How employee what to protect: employees must be taught to know what type of assets need protection and at what level in the organization.

Simplify best practices: best security practices involve creating strong password and safe browsing on the internet.

Teach the principle of persuasions: It cannot be predicted on how cyber criminals will attack the systems in an organization hence it is important to insure that a least employees understand the techniques that social engineers use to manipulate people so that they recognize social engineering attacks coming in the form of email, phone call and unannounced visitor.

2.8 Information security frame works

2.8.1 ISO/IEC Standards

Organization should comply to ISO/IEC Standards like 27001:2013 as there are very important components outlined that can help address the human factor threat to information security other than depending on technical controls. ISO standards are designed in agreement with international standards hence, it is ideal as organization can adopt comprehensive security strategy especial in this digital era where cyber threats are prevailing issues (Information Security Expert Group, 2016). Figure 10 illustrate the components of ISO/IEC 27001:2013 guidelines.

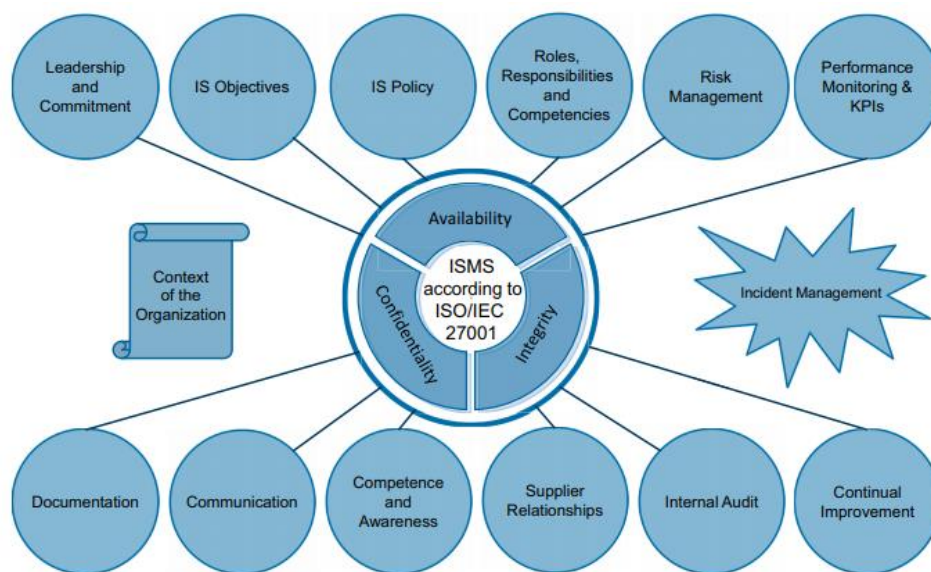


Figure 10 ISO/IEC:27001:2013: Source: (Information Security Expert Group, 2016)

Information risk management (IRM) frameworks

IRM are documented processes and procedures to enable organization effectively address risks associated to information and assets with cost effective measures to avoid incurring higher costs (Landess, 2003). It worth noting that risk is a future event that can affect the business function and subsequently fail to achieve its financial goal. It is also worth noting that organizations work hard to insure core security elements such as confidentiality, integrity and availability are not compromised (Landess, 2003). Hence, IRM frames works enables employees to reflect on whether strategies used in risk management activities to protect CIA in a company are carried out effectively and efficiently. Risk management process includes, monitoring risk, access to updated information, decision making process supported by standardized frame works of risk analysis and evaluation. Information risk is the negative

effects on business due to loss of the CIA of information (Landess, 2003). Figure 11 Illustrate definition elements of IRM.

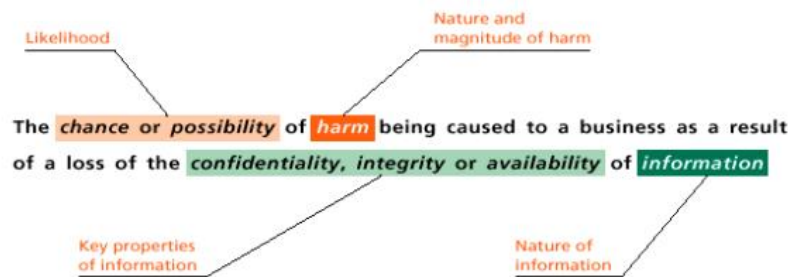


Figure: 11 Defining elements of IRM: source (Landess, 2003)

It worth noting that a Risk Management Process Model can also be a useful tool that enable decision makers to identify risks to information security and reach an agreement on security controls required keep the risks within allowable threshold. (Landess, 2003) outlined the following components of risk management process as follows.

Identify: This component entails identification of actions that are may result in risky to information.

Analyze: This component entails assessing, establishing measurements and prioritizing of threats and vulnerability to information security so that the right security control is adopted in the organization.

Control: a security controls such as formal or informal policy, method, or procedure that help to counter the identified threats and vulnerability to information security.

Monitor: practical actions such as assessing and evaluating performance of security controls in order to take corrective measures.

Report: entails actions taken such as informing the management about threat and vulnerability with accurately by outlining the events happened with detailed information

Contingency Planning CP

CP: Is a reactive measure that entails a process of preparing for unexpected events that might affect business operations in an organization (Awan 2006). It entails how management in an organization align themselves in order to get ready and react immediately to threats before escalating further in an organization (Awan 2006). The components of CP include;

Incidents Response Planning (IRP): focuses on urgent responses to incidents.

Reports from user combined with reports from intrusion detection system can help in establishing the nature of incidents in an organization (Awan 2006). Incident indicators to information security includes execution of unknown programs, unusually system crashes, availability of unfamiliar files and unusual consumption of system resources. Figure 12 below illustrates incident response after the incident.

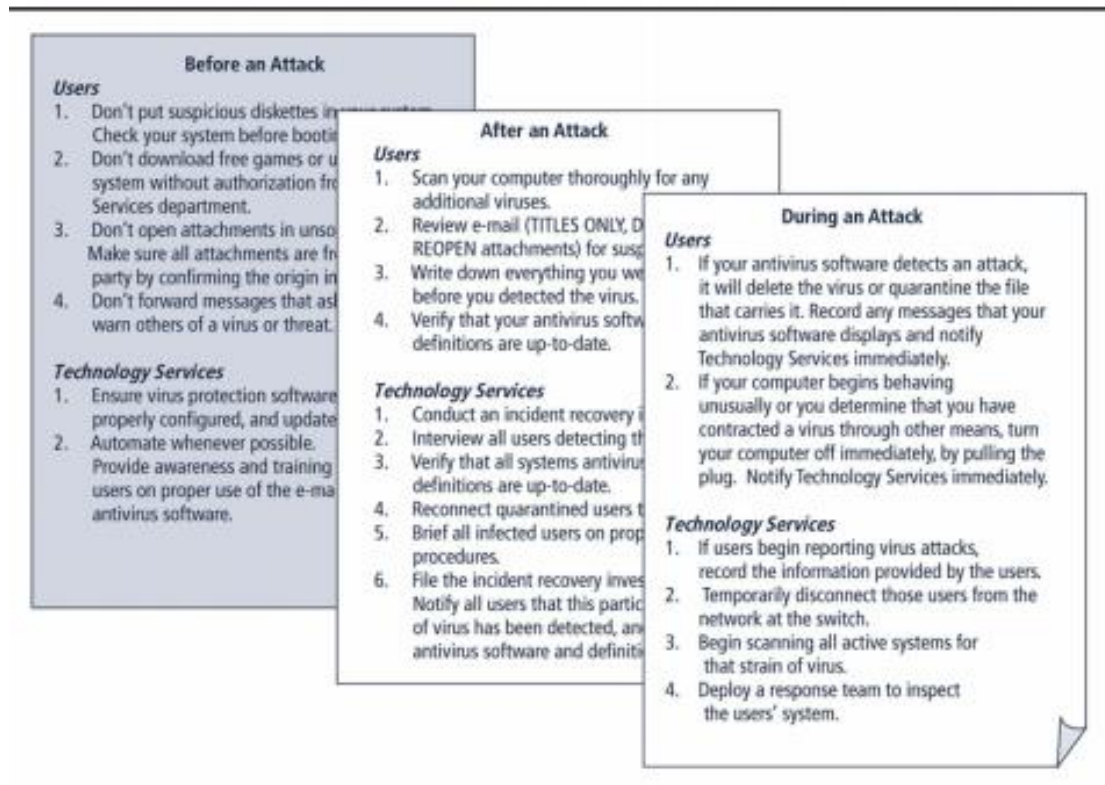


Figure 12 Incidents response by users: source: (Awan 2006)

Business Continuity Plan (BCP): Focuses on other alternative measures to enable business operation continue in case a disaster strikes.

Disaster Recovery Planning (DRP): focuses on recovering business operations after being hit by disaster. DRP procedures are implemented if a company had failed to contain the damage on information and assets which severely affects business functions from continuity. Awareness of the possible risk of disaster and its mitigating strategy is important to be communicated among employees (Mokhopadhyay and Bhattacharjee, 2015).

2.9 Theoretical Research Models

Theoretical models help understand the situations being investigated and provide support to the aims, objectives, problems statement and research questions of the study (Grant and Osanloo 2014). In order get insights about End User behavior, attitudes and knowledge towards information security, the Theory of Planned Behavior (TPB), Technology Acceptance Model (TAM) and Protection Motivation Theory (PMT) were used in the study.

2.9.1 Protection Motivation Theory (PMT)

(Rajendran and Shenbagaraman 2016) studied that PMT is widely used in the field ICT to investigate security lapses. (Rajendran and Shenbagaraman 2016) added that PMT has been applied in the Adoption of Protective Technologies, which tends to avoid destruction from increasing threats such as malicious software's. (Janmaimool, 2017) asserted that PMT takes into consideration the decision taken by a user to take part in risk preventative behavior based on their motivation to defend themselves from threats. PMT was developed by Ronal Rogers and was original developed to be applied in health related research (Hindle and Clubb 2015). The PMT is commonly applied in information security or cyber security to appeal fear on the consequences of taking a particular action. PMT consist of two cognitive process such as threat appraisal and coping appraisal (Jansen 2015). For example, web browser like Google Chrome display warning alerts in red and messages like your connection to this site is not private are meant to instill treat appraisal. Other concepts which have been adopted from the PMT model include password expire warning, email warnings like Gmail account is under spam attack and antivirus warnings flushing in red color so that users can take safety precautions to protect information from anticipated risk. The fear appraisal is a tool of persuasion meant to call attention and motivates action. Based on this theory, it therefore hypothesized that;

H1 End users with information security aware are more attentive to security controls than end users who are not information security aware.

H2 End users with information security awareness are more attentive in changing their password than users who are not information security aware.

H3: An organization that educate its employees regarding its policy is less likely to experience issues of none compliance than an organization that does not educate its employees about its security policy.

H4: An employee is aware of threat to information is likely to report suspicious activity than an employee who is not aware about threats to information security.

2.9.2 Theory of Planned Behavior (TPB)

The TPB is adopted in the field of IS to help researcher explain the connection between attitudes, knowledge and behavior with respect to the use of computers (Warkentin, Malimage and Kalana, 2012). Therefore, TPB can be used to establish the influences of employee behavior, attitudes and knowledge on security controls adopted by the organization (Denev and Hu, 2007). Security controls is a collection of technologies that is used to counter threats in an organization such as unauthorized access, virus and intruders. Employee's behavior can be influenced by their intentions to engage in the behavior of their interest. Behavioral Intention to obey security policies was found to be significantly influenced by attitudes of employees towards security policies (Warkentin, Malimage and Kalana, 2012). TPB outlines that intention to engage in a particular behavior is determined by 3 factors namely Attitude towards the behavior, Subjective Norm and Perceived Behavioral Control (Kranz, Kolbe and Muntermann 2015). The TPB is also linked to information security to determine the likely hood End User engages in risk behavior that can contribute to information security breaches. This includes but not limited to the likely hood of a user clicking on a phishing link, spam or install Trojan horse. TPB model helps to establish Personal attitudes of a user to the behavior by identifying their outcome belief for taking the behavior. Outcome belief and outcome evaluation cause an individual's personal attitude. Attitude can be positive or negative. The TPB can be of great importance in finding out the Subjective Norm which refers to own opinions of what is normal to an individual and it comprises of normative beliefs and motivation to comply. Normative believe is all about the information that individuals obtain from other people through different sources of information like security awareness. Motivational to comply implies to how motivated users to responds to messages they receive in order secure information (Denev and Hu, 2007).

Personal control believes is made up of self-efficacy beliefs and perceived external beliefs. Self-efficacy reflects on the level of confident an employee has to achieve change even if there are some obstacles. Perceived external are those factors that can prevent users from achieving their goals.

Attitudes towards the behavior raises questions like does an individual believes that certain behavior makes a positive or negative contribution towards the person life. For example, does clicking on a particular unknown link makes sense for an individual.

The Subjective Norm gives an insights surrounding an individual on cultural norms such as security guidelines adopted by the organization (Kranz, Kolbe and Muntermann 2015).

Perceived Behavioral Control: gives an insight of how an individual can easily express certain behavior or act in a particular manner towards security controls adopted by an organization. Figure 13 illustrate TPB

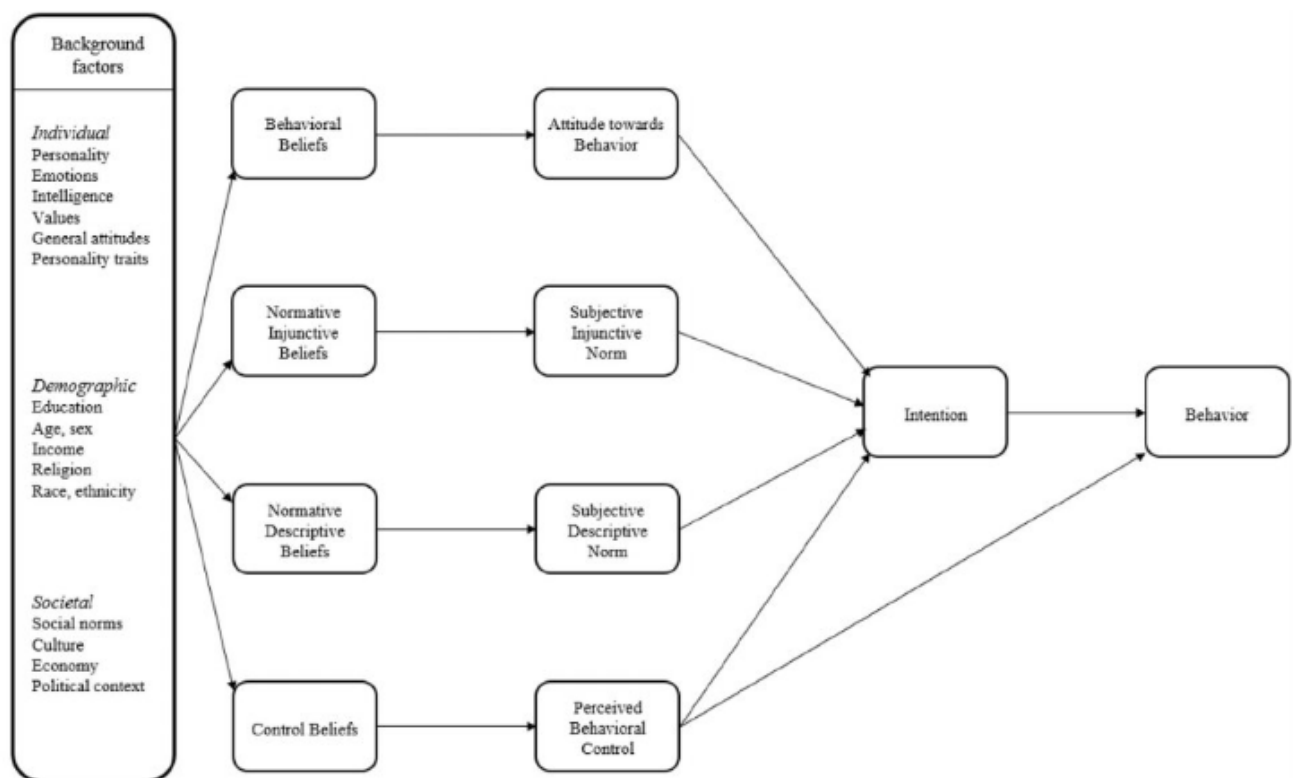


Figure 13 Theory of Planned Behavior. Source: (Leeuw et al, 2015)

An employee's intention to carry out an activity is particularly determined by personal Attitude, Subjective Norm and personal Control beliefs. Attitudes are the best predictors of forming a Behavioral Intention. If an individual believes that the construct is unfavorable, she/he is not likely to take action (Denev and Hu, 2007). Based on this model, it is therefore hypothesized that

H3: Employees who are aware of the importance of security controls in an organization are less likely to make information vulnerable to cyber-attack.

H4: Employees with negative attitudes towards protection measures put in place are likely to engage in risk behavior which might compromise information.

H5: Employees with lack of ISA are likely to compromise information security.

2.9.3 Technology Acceptance Model (TAM)

The TAM model is widely used to explain end user acceptance behavior on new technology adopted by an organization and it was introduced by Davis in 1986 (Ma and Liu 2014). The theory suggests an individual intention to acknowledge the use of a particular technology depends on an individual attitudes regarding its use (Kranz, Kolbe and Muntermann 2015). The construct in this model includes perceived Usefulness (PU), Perceived ease of use (POEU), attitude and behavioral intention to use. PU and POEU constructs are well related to end user beliefs on the use of technology and hence they are useful to predict user attitudes towards the technology which eventually assist to predict the level a user acceptance to the new technology in an organization (Ma and Liu 2014). PU can be linked to how a particular technology can improve employee performance in an organization and POEU implies that security controls should be easier to use by employee to enhance information security. TAM is adopted in the field of information security such as technical countermeasures like the use antivirus. PU requires that employees understand the drawback of complying with IS policy in an organization. Based on this model, it is therefore hypothesized that

H6: Training and education among employees is likely to reduce security breaches in an organization.

H7: knowledgeable employees on security controls are likely to enhance information security in an organization.

CHAPTER 3

Research Design and Methodology

This chapter also illustrates how research samples and questionnaire were defined in line with the literature review and the research questions in order to establish the relevant responses from participants.

3.1 Quantitative

Quantitative research approach is the use of statistical data to measure the results of survey (Daniel, 2016). Information gathered from participant's responses on each questions were analyzed and translated into figure which were presented into table, bar graph and pie charts. Quantitative data can be measured easily as compared to qualitative data. It was also ideal to use quantitative data because structured questions were used as opposed to unstructured questions which is suitable for qualitative data.

3.2 Sampling

In this study, stratified random sampling was used to come up with a sample size from different branches of the university. Gaborone University College of Law and Professional studies (GUC) has 7 branches in Botswana. A sample size of 42 was selected but only 32 participants were investigated. A non-probability sampling approach was selected due to limited resources likes time, money, workload and the approach was ideal to explore people behaviors on protection controls. Sample sizes were defined as illustrated on Table 3.

Table 3 Population sampling

Organization Branch		Stratum
	Branch 1	Stratum 1=7
	Branch 2	Stratum 2=7
	Branch 3	Stratum 3=7
	Branch 4	Stratum 4=7
	Branch 5	Stratum 5=7
	Branch 6	Stratum 6=7
Total		42

Within each stratum, a Simple Random Sample (SRS) of 7 was selected and the SRS were combined to get a full sample. A total research population of 42 participants was targeted. The results from different branches were aggregated so that each branch had an equal weight regardless of the achieved sample size in each branch.

3.3 Data collection

Secondary data and Primary data were used in the research study. Secondary data refers to information collected from existing literature already been done by other researchers and published for reviews by others (Osang et al. 2013). Primary data refers to raw data that is collected by researcher from the source (Osang et al. 2013)

3.3.1 Secondary data: The following sources of information were used in the research study to acquire knowledge on how the human factor impacts on IS controls and possible solutions; books, magazines, journals, conference papers and electronic databases.

3.3.2 Primary data: firsthand information about employee knowledge, behavior and attitudes towards security controls and demographic data was gathered for further analysis.

3.4 Data collection instruments

Data collection instruments used in the survey includes the following

3.4.1 Questionnaire

A questionnaire is a tool that can be used to collect information from participant regarding their social characteristics which entails their behavior, attitudes, beliefs and their actions to be used in addressing the problem (Bird, 2009). In order to establish the level of ISA among end users in organization, structured questionnaire was prepared and some were physically handed to participants and some were send online. A questionnaire was used in the research study because it was cheaper to administer as compared to interviews (Mathers, Fox and Hunn, 2009). The questionnaire was also selected due to limited resources such time and finances. A structured questionnaire was designed that contained 33 questions and it was redefined via two alterations of pilot testing on a smaller number of participants before it was distributed to selected participants. Pilot testing was done to verify errors and establish if the questionnaire will capture the right answers for the research questions. Other methods of collecting data such as interviews were not used due to the limitation that, interviews are labor extensive and telephone interview was not possible as participants were on busy schedule and cannot be accessed on telephone (Mathers, Fox and Hunn, 2009). See appendix A for illustration of the questionnaire

3.5 Ethical considerations

Ethical issues related to the research topic were highly observed to protect participants' anonymity, privacy and confidentiality of information (Makau and Akaranga 2016). Participants were provided with information consent letters before they were provided with questionnaire. Participants were assured that the information provided shall be used for the purpose of the study in order to instill trust with participants because the topic included some aspects of information security (Makau and Akaranga 2016). Some of the contents of the information consent letter detailed that participant will not be forced to respond to the questionnaire study as illustrated in Appendix C. However ethical issues related to research study such as fabrication, plagiarism and falsification were also observed.

CHAPTER 4 RESULTS

The first section of this chapter focus on an outline of information gathered from participant's responses. Data measurements used include password management, Unknown Email links and attachments, demographic data, physical security and technical security control. The survey attained a response rate of 76% that is, 42 questionnaires were sent to the participants and out of 42 only 32 participants responded. Data from questionnaire was captured into excel for further analysis using excel features such as Pivot tables and charts. The questions were coded as illustrated in Appendix B. Participants response results on their level ISA were presented as follows:

4.1 Demographic Data

Demographic data was collected in order to understand the research population distribution such as age, gender and their educational background.

Gender: The gender distribution shows that 69% of participants were female and 31% of the participants were males. Figure: 14 illustrate employee gender distribution

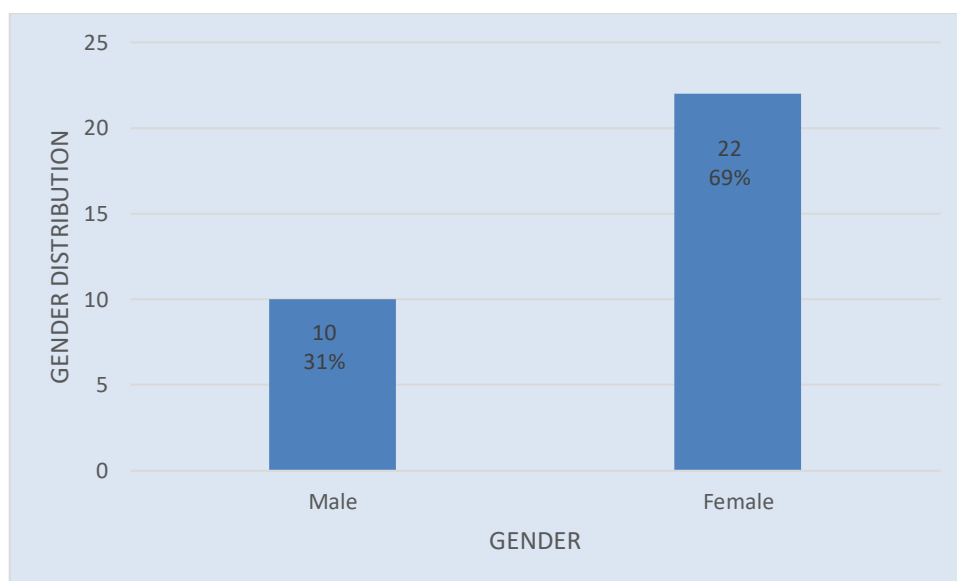


Figure 14 Gender distribution

Age: The results show that 60% of participants in the organization are within the age range 31-40, 18% are in the age range between 21-30, 16% are within the age range 41-50 and 9% of participants are within the age range of 51 and above respectively. Table 4 illustrate the respondents' age characteristics.

Table 4 Participant's Age characteristics

AGE	21-30	31-40	41-50	51 and above
Total number of employees within age range	6 18%	18 56%	5 16%	3 9%

Educational background: The results of the research study shows that 53% of participants have post graduate or Doctorate qualifications and 47% of participants have Higher Education within the bracket of Diploma and degree respectively as illustrated in figure 15

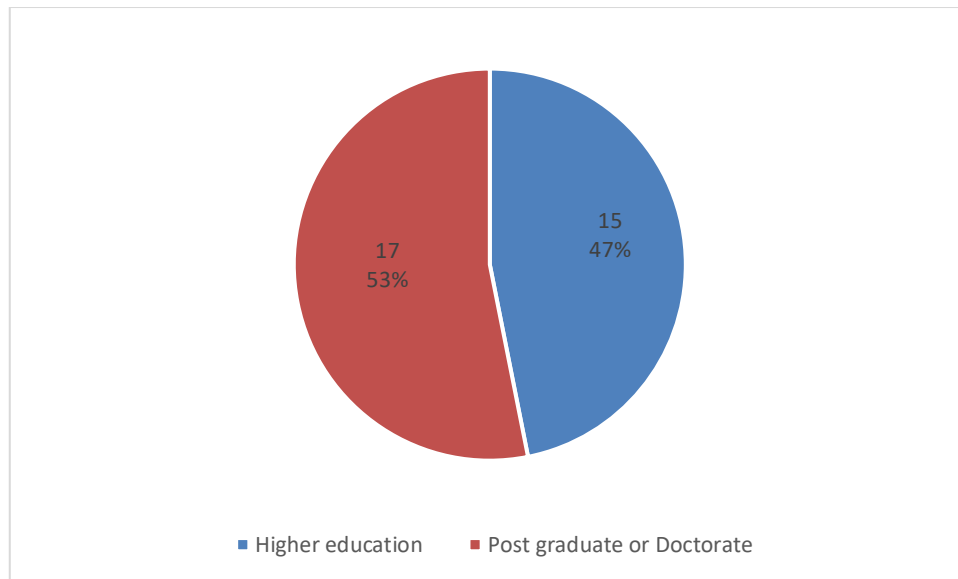


Figure 15 Participants educational background

Field of study: The study shows that 81% of participants have qualifications which are Non ICT related and only 17 % of participants have qualifications which are related to ICT. Figure 16 illustrate participants field of study.

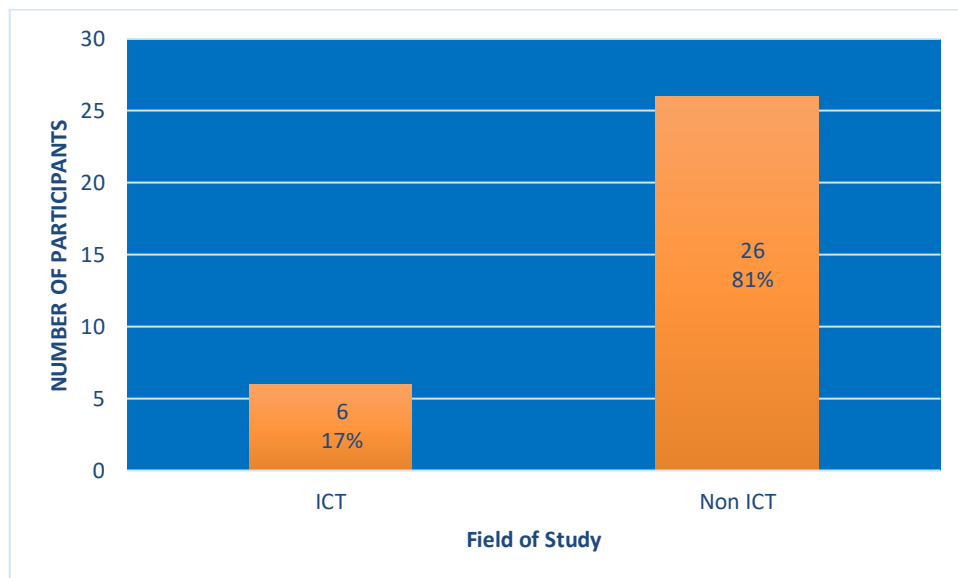


Figure 16: Participants field of study

4.1.2 Password Management

A password is used as first line of defense to protect Information Systems. The result shows that 67 % of participants use a password and username as a form of authentication and 34% do not use a username and a password. It was established that 59% of participants have shared their password and 41% of participants have not shared their password. It was also noted that

62% participants memorize their password, 16% of participants write their password on paper and 22% of participants save passwords in their cellphone. Figure 17 illustrate participant's responses on password security.

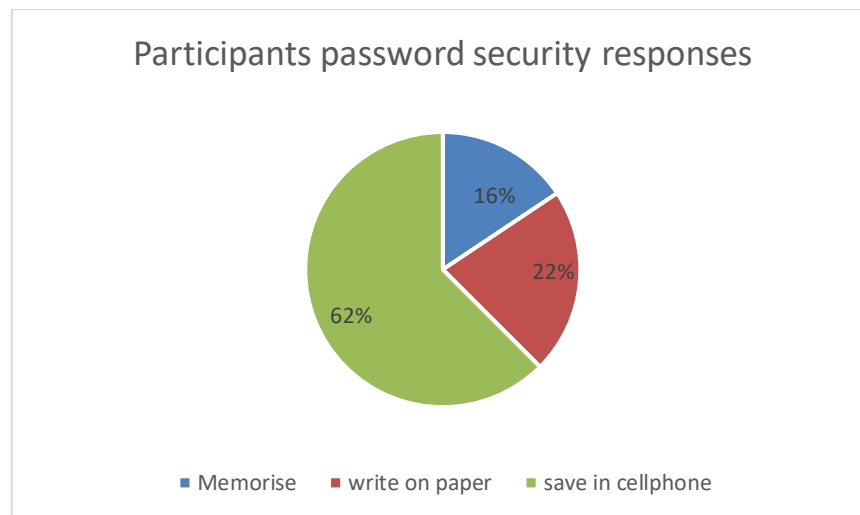


Figure 17 participant's responses on password security

It was found out that 75% of participants use the same password to log in to different systems and applications and 25 % different passwords to log into different system or application. The results further show that 53% of the participants create password length of 8 characters, 25% of participants use 14 characters, while a minimum of 13% of participants use 4 characters and 9% of participants create passwords of up to 5 characters respectively as illustrated in Table 5

Table 5 Participant's password length distribution

Password length	Number of participants	Percentage
4 characters	4 out of 32	13%
5 charters	3 out of 32	9%
8 characters	17 out of 32	53%
14 characters	8 out of 32	25%

It was found out that 59% of participants create a password from a combination of symbols, numbers and special characters while 41% of participants do not use a combination of symbols,

numbers and special characters. The results also show that 59% of participants change their password and 41% do not change their password.

4.1.3 General threats to information security and internet use

General security consciousness of employees towards the use of the internet, emails and general knowledge on threats to IS was established. The results show that 34% of participants have excellent understanding of information security, 41% of participants have good understanding of information security and 25% of participants have average understanding of information security. With regard to knowledge of threats to IS, it was found out that 53% of participants have low knowledge on threats to information security, 31 % have moderate knowledge and 16 % have high knowledge on threat to information security as illustrated on Figure 18.

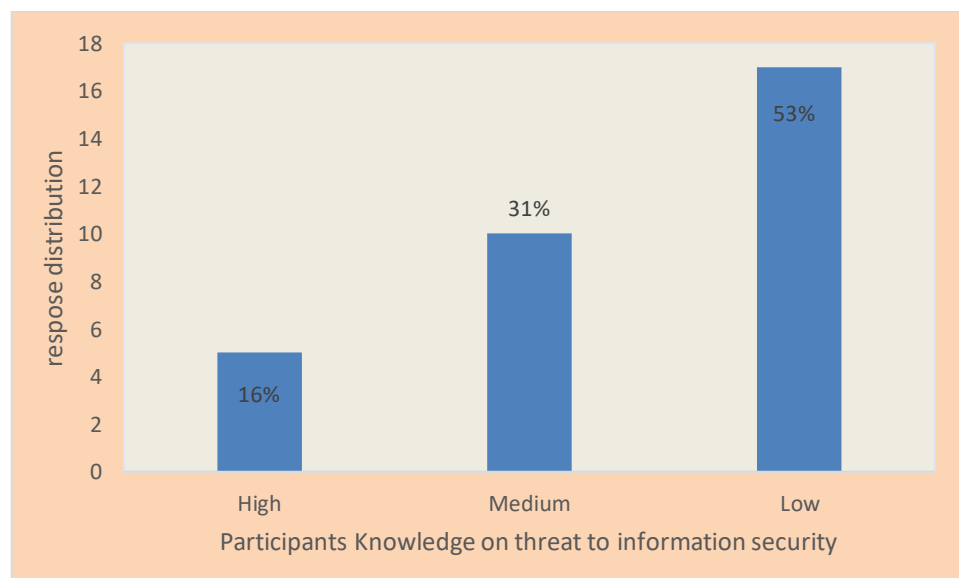


Figure 18: Participants knowledge on threat to information

It was found out that 84% of participants have downloaded email attachments from unknown source and 16% of participants are not sure if they have ever downloaded email attachment from unknown source. The results show that 88% of participants do not encrypt emails messages before sending it over the internet. It was established that at least 31% of participants have not forwarded email suspected to be spam to their colleagues while 38% have never and 9% of participants were not sure if they had forwarded an email suspected to be spam. It was also established that only 38% of participants confirm whether the email is indeed from an employee who left the company before reading the contents and 63% do not confirm before

they open the e-mail and read. It was established that 50% of participants report immediately on incidents of malicious activity in their email accounts, 22% of participants observe the situation, 16% of participants try to log into another computer or restart the computer. 72% of participants do not confirm if the website they access is secure and only 28% do confirm.

4.1.3 Technical Security Control

It was interesting to discover how some participants responded on who should take measure to stop the spread of computer virus, fraudulent emails, spyware and spams as illustrated on Table 6

Table 6 Participant's responses on measures to stop the spread of malicious software's

Option	Employee response	Percentage rate
Internet Service Provider	2	6%
Antivirus Software Companies	12	37%
Computer Software companies	6	19%
System administrator	12	38%

It was established that 84 % of participants do not know the type of antivirus installed into their computers and 16% of participants know about the antivirus installed in their computer. It has also been noted that 72% of participants do not scan their USB drive and only 28% scan USB drive before opening. Most participants 69% opt to restart their computer when they encounter pops messages like restart your computer to install important updates and it was discovered that only 31% ask for help. It was found out that 72% of participants do not logout on computer when they are called for meetings and only 28% logout on computers.

4.1.4 Physical Security Control

Information security is not all about the use of computer software to protect data hence an insight on how employees perceive the importance using physical security measures to protect organizational assets was considered. It was found out that 59% of participants do not power off computers after working hours and only 41% of participant's power off computers. It was noted that 63% of participants are not aware how to use fire extinguisher in case of emergency

and at least 37% employees are aware. It was also established that 81% consider security cameras are important than a guard man whereas 18% of participants consider guard man are important as compared to security cameras.

4.1.5 Organizational security policy

It was noted that 50% of participants disagreed with an aspect of establishing a policy to restrict downloads and use of external drive and 31% strongly disagreed whereas, 19% slightly disagreed. It also was found out that 43% of participant's backup data and 56% do not backup data. The research study also established that almost all participants have never participated in security awareness programs. Lastly the result show that 66% of participants are aware of security policy established in the organization and 34% are not aware of security policy in the organization.

CHAPTER 5 DISCUSSION

According to the survey, there are more female employees as compared to males in the organization which suggests that the organization promote gender equality in the workplace. Majority of employees in the organization are within the age range 31-40. Employees within these age group (31-40) can easily adhere to security controls (Hadlington, 2018). It is also commendable age group because employees still have the energy to work under pressure to produce good results for the organization. However, 34 % of employees below the age of 31 are likely to place the organization at increased threat from malicious attacks likely due to the reasons that it will be difficult for them to cope with security policy that prohibit file downloads from unsure websites (Hadlington, 2018).

It is quite interesting that the organization have at least employees with masters and Doctoral degree even though there is a slight percentage increase of 6% from employees with Higher education. Employees with higher educational qualifications is advantageous for the organization because educated individuals can easily acknowledge the significance of security controls implemented to safeguard information in the organization (Rainer and Harrison 1992). However, it is worth noting that the majority of employee's educational background is not in the field of Information Communication and Technology (ICT) which can also place the organization Information Systems to increased cyber threats in cases where ISA is not raised as shown by the research findings. It is also likely computer incidents in the workplace are

likely to occur which might compromise information security. It was established that 53% of participants have low knowledge on threats to information security which is consistency with the higher number of employees from none ICT related field and 25% of employees with an average understanding of what information security entails which might also place the organization vulnerable to cyber security threat such as phishing attacks.

The finding has also revealed that there is lack of security consciousness among some employees in the organization because, they because share password. Sharing password is not a good security practice because chances of a shared password being compromised are higher which can put information and systems into danger of unauthorized access (Chareon, 2014). A password is used to prove identity before a user can gain access into the system and as a result another user with a compromised password can claim to be a legitimate user and gain access into the system and steal confidential information, disrupt and delete important files (Blazevic, Ocevcić and Solić 2015). According to the data collected it shows that almost the majority of end users 75% uses password length of fewer than 10 characters. However, password with fewer than 10 characters can be easily cracked by hacker using dictionary attacks (Chareon, 2014). According to the survey, 62% of employees memorize their password which is good depending on how often they use the password. However, chances of forgetting the password cannot be ruled out which might increase log on issues in the organization. some employees write their password on papers which is not a good security practice because such behavior increases chances of the password being compromised and a similar issue also applies to 22% of employees who save their passwords on cellphone because if the cellphone is lost, chances of the password being compromised are high. Almost 75% of employees use the same password to log in to different systems or application which is also not a good security practice. If the password is compromised, all the systems that the user have access with the login credentials will be compromised.

Risky behavior is common among employees taking up a larger percentage rate of 80% to have downloaded email attachments from unknown source. Risk behavior to information security is any activity that subject an employee or the organization to cyber-attacks such as downloading copyrighted materials from illegal websites (Hadlington, 2018). Security conscious is important among employees and contrary to this, there is lack of security consciousness among employees with at least 60% employees are likely to be phished because they never confirm the source of emails message before opening and if the web site they access are secure. Phishing is a strategy used by attackers to deceive end users (Sumari, Alomari and Rajalingam 2012).

employees do not encrypt confidential information before sending it over the internet. Sending important electronic message without encrypting the data is not a good security practice and it can place the organization into threats such as identity theft. Some employees feel that emails from employees who left the organization are always legitimate and they accept links without confirming the sources details. It is very risk actions as noted by (Probst and Hunker n.d.) that disgruntled former-employees can harm or destroy confidential information by taking advantage of employees who are not security conscious within an organization.

There is also a pattern of risk behavior that was noted among employees as the survey findings shows that 60% of employees do not scan USB flush drive before they access the storage. it is not a good security practice to open external drive like USB flush drive since 25% of malicious software's like virus, spyware is transmitted through portable devices (Walters 2012).

According to the survey, almost 72% of employees in the organization do not logout on the computers when called for staff meetings hence creating opportunity for intruders to gain access to unauthorized information. An intruder can do a lot of harm to information and system such as disconnecting network cables which can affects the property of information such as availability. An intruder can also physically steal computers. It is also notable that the majority of employees are not aware of the type of antivirus installed into their computer which suggest that they are likely to ignore important updates and disable firewalls settings that is helpful in detecting malicious software. It is a good security practice to report suspicious activity however, employees do not report malicious activity instead they decide to take actions such as restarting the computer when they encounter unusual system popups without asking for help. As a result, employees are likely to fall victims of social engineering attacks. Cyber criminals design fake system updates in order to deceive end user and eventually compromise information systems (Sumari, Alomari and Rajalingam 2012). Information Systems becomes vulnerable to intruders who can steal confidential information and inject Trojan horse to secretly gather information on Information Systems. Some employees in the organization do not backup data. Data backup is important strategy to recover files in case of system crashes and other incidents such as fire and flood. The is lack of knowledge among employees on the use of physical control like fire extinguisher in case a disaster strikes. Some employees in the organization do not switch of computers after working hours. Employees have divergent views on the importance physical security controls like installation of security cameras and a security guard man.

CHAPTER 6 CONCLUTION

The research study was an effort to contribute in the field of information security research particularly the human issue in organization. The findings show that what was hypothesized is consistency with the results and the research questions of which it was found out that, there is lack knowledge on threat to information security as well as understanding of what is information security among employees in the organization. Some employees believe that protecting information systems from malicious software's is the responsibility of Internet Service Provider (ISP) while others believe that is the responsibility of company which sells software's. Employees in the organization engage in risk behavior such as sharing password, using the same password to log in different systems and applications. The is lack of security consciousness among employees as evidenced by high number of employee who access, download files from unknown source and unsecure websites which is a huge compromise to main goals of security such as CIA. Security policy is an important tool that can be used to protect information hence employees must be aware of its importance in the organization. security awareness can help mitigate insider threats but the study show that majority of employees have not attended any security awareness program.

CHAPTER 7 RECOMMANDATIONS

Raising awareness in the organization

There is a need to raise ISA among employees in order for them to be aware of the nature of malicious and none malicious acts which can threat security goals of an organization (Khan et al. 2011). ISA among employees will enhance understanding on the importance of security controls adopted by an organization (Metalidou et al. 2014). Awareness should be focused on the following areas:

Password Handling and usage

Employees should be encouraged to use password of more than 8 characters or create strong password. Shorter password can be easily hacked using dictionary attacks and other password cracking tools (Solic, Nenadic and Galic 2012). Employee should be encouraged to use password management tools like KeePass and Apple's iCloud Key to store password safely and help in case a user forgets the password. Employees should be encouraged to avoid sharing

password to reduce the risks of intrusion and Social engineering attack. Social engineering attack can be prevented by not sharing personal information to the sender unless the receiver has verified the authenticity of the sender (Yadav Kumar and Chandel 2017). Employees should be encouraged to use software tools like Key Scrambler, Spy shelter to prevent key logger and phishing attack (Yadav Kumar and Chandel 2017). The organization should adopt other none technical approach to address issues related to password handling and lack of security consciousness like vetting new employees, continuous monitoring of behavior and compliance to ISO/IEC Standards. It is worth noting that the organization should introduce a password policy and awareness must be conducted so that employees can understand its significance in enhancing computer security.

Malicious Protection

Employees need to be encouraged to avoid downloading from websites which are not secure to avoid threats such as virus and Trojan horse. Employees must be encouraged to update antivirus and the importance of updating antivirus should be emphasized. The organization should consider documenting Internet usage policy to regulate its network, equipment and internet access.

Employees should be encouraged to consider the importance security policy established in the organization as administrative tool used to protect information and other assets in the organization. Employees should not view policy as tools used by the management to keep track of employee's activity and evading their privacy. employee's knowledge on computer related security, compliance and procedures is important (Karwowski and Glaspie, 2018). The organization should also consider adopting Contingency plan like IRP, BCP and DMP. Incident Response Policy helps to urgently react to acts of malicious activities to enable users take actions like isolate: disconnect system from a network and report the incidents.

Email attachments and unknown source

Employees should be encouraged to be security conscious when downloading attachments from unknown source to avoid falling victims of keystroke logging attacks. If user key inputs are captured by an attacker, login credentials can be compromised. File attachment is a method that is commonly used by cyber criminals to execute Trojan horses to gather information about user activity in the systems without their knowledge. Attackers send fake email messages that lends on legitimate user's inbox that looks like they are from trusted websites belonging to

known financial banks and educational institutions requesting a user to provide their personal information hence employees should avoid using unknown links. The organization should consider access control mechanisms that support CIA. The organization should consider installing Pretty Good Privacy (PGP) on computers used by its employees. An awareness should also be conducted on the use of PGP so that employee understands the importance of using PGP to secure emails. Users can generate their own PGP key that can be used to encrypt email message before sending to the other party and decrypt email messages upon arrival to the destination (Hostiad and Surdama 2016).

Physical access

Employees should be encouraged to lock doors and shred documents not in use after working hours to keep away from intruders. Awareness on physical protection must be raised among employees since majority of employees do not know how use emergency tools like fire extinguisher. Awareness on the importance of multiple layered defense should be raised among employees since other employees consider security cameras are important than security guard. A weakness on physical security control can impact negatively on information security.

System shut down

Employees should be encouraged to shut down or lock computers when called for meetings and other office engagements. If an intruder like another employee with malicious intentions find the computer unattended, they can steal, delete important files and even change the system password to avoid traces.

Social engineering attacks

Employees should be careful of social engineering attacks because, cyber criminals often use messages or information that an innocent employee can easily be deceived to believe that the information is legitimate. Design phishing emails and pop-up windows by incorporating official logos, web site design from real organizations and other information of interest that can be used to deceive end users (Sumari, Alomari and Rajalingam 2012). Hence it is important that employees should be encouraged to be security conscious whenever they are online.

The organization should consider the following awareness tools

- Electronic mail messaging
- Group discussions

- Computer aided training
- Posters

The organization should also consider designing an awareness program. Awareness program is an important tool that can be established in order to close the gap such as lack of security consciousness among employees as suggested by (Hash and Wilson, 2003).

Further research

In order to explore the human issue further, the research scope should be extended to include Management and students in the organization. More analysis on the organization's security posture should be established to find out if it is in accordance with ISO/IEC Standards. The research study was conducted on one tertiary institution in Botswana hence in future the scope should be extended to included other tertiary institutions.

Limitations

Some of the participants did not respond to the questionnaire which was distributed and these affected generalizability of results. There were some challenges encountered when collecting the questionnaire because the time frame agreed with participants to have completed the questionnaire was not met since some of the participants requested to extend the time to complete the questionnaire as they were busy with logistics for students who were writing exams. It was also realized that the field comments in the questionnaire could have been included so that participants can suggest their views because some participants did not attempt some of the questions which affected analysis of the findings. Interviews were not conducted as the participants were engaged with their duties. The study intended to develop a phony phishing system for experimental purposes to validate the findings. However due to time constraints this could not materialize. See appendix D for a drafted phishing form developed using HTML.

LIST OF REFERENCE

1. Goutam. R. (2015). Importance of cyber security. International Journal of computer applications. Vol 111 (7).
2. Valiente. C. (2016). Addressing malware with cyber security awareness. Developing and connecting cyber security globally.
3. Badie. N and Lashkari. A (2012). A New Evaluation Criteria for Effective Security Awareness in Computer, Risk Management based on AHP. Journal of Basic and Applied Scientific Research.
4. Gao. X, Yang.Y, Liu. C, Mitropoulos. C and Lindqvist (2018). Forgetting Password Ecological Theory and Data: The Advanced Computing Association 27th Security USENIX Symposium.
5. Rajalingam. M, Alomari. S and Sumari. P (2012). Prevention of Phishing Attacks Based on Discriminative Key Point Features of Webpages. International Journal of Computer Science and Security. Vol 6 (1).
6. Denev. T and Hu. Q (2007). The Centrality of Awareness in the Formation of User Behavioral Intention Towards Protective Information Technologies. Vol 8 (7).
7. Schulze. H (2018). Insider Threat. Cyber Security Insider Report.
8. Cherdentseva. Y and Hilton. J (2013). A Reference model of Information Assurance and Security.
9. Landess. D (2003). A Practical Information Risk Management Process. A Global Information Assurance Certification (GIAC) Security essential version 1.4b
10. Maingak. A and Harsono. C (2018). Information Security Assessment; Using ISO/IEC 27001: Standard on Government Institution. Vol 17 (1).
11. Beyer. R and Brummel. B (2015). Implementing effective cyber security training for end users of computer networks.
12. Sommestad (n.d). Human factors related to the performance of intrusion detection operators. Department of information and Aeronautics Systems, Swedish Defence Research Agency (FOI).

13. Hadligton. L (2018). Employee Attitudes towards Cyber Security and Risky Online Behavior: an empirical assessment in the United Kingdom. *International journal of cyber criminology*. Vol 12 (1).
14. Colwill. C (2009). Human Factors in Information Security. *Information Security Technical Report*. 14 (186-196).
15. Battele (2015) How to Implement Security Controls for an Information Security Program. United Nations Interregional Crime and Justice Research Institute Reports.
16. Leeuw. A, Valois. P, Ajzen, and Schmidt (2015). Using the theory of planned behavior to identify key beliefs underlying pro-environmental behavior in High School students. *Journal of Environmental Psychology*.
17. Jouini. M, Rabai. L and Aissa. A (2014). Classification of Security Threat on Information Systems. 5th International Conference on Ambient Systems, Networks and Technologies (ANT).
18. Werlinger. R, Hawkey. K and Beznosov. K (2008). Human, Organizational and Technology Challenges of Implementing Information Security in Organizations. *Proceedings of the second international symposium on human aspects of information and security assurance*.
19. Cengage Learning (n.d). *Introduction to information security*.
20. Information Security Expert Group (2016). *A Practical Guide for Implementing in accordance with International Standards ISO/IEC 27001:2013*. Information System Audit and Control Association (ISACA).
21. Mokhopadhyay. B and Bhattacharjee. B (2015). Use of Information and Technology in Emergency and Disaster Management. *American Journal of Environmental Protection*. Vol 4(2).
22. Norman. A and Yasin. N (2010). A critical review of information systems security management (ISSM) implementation: Comparison between stable organizations and emergent organizations. *International Journal of Digital Society*. Vol 1 (3).
23. Ugbogbo. N and Michael. A (2016). Ethical Issues in Information and Technology. *Journal of accounting*. Vol 2
24. Choi. M, Levy. Y and Hovac. A (2012). The role of User Computer Self-Efficacy, Cybersecurity Countermeasures, Awareness and Cyber Skills Influence on Computer Misuse. *WISP Proceedings 2012*.

25. Amarachi. A, Okolie. O and Ajaegbu. A (2013). Information Security Management Systems: Emerging issues and prospect. *Journal of Computer Engineering*. Vol 12 (3).
26. Shareef. S (2016). Enhancing security of information in e-government. *Journal of emerging trends in computing and information science*. Vol 7 (3).
27. Chan. H and Mubarak's (2012). Significance of Information Security Awareness in Higher Education. *International Journal of Computer Applications*. Vol 60 (10)
28. Khan. B, Alghathbar. K, Nabi. S and Muhammad. K (2011). Effectiveness of Information Security awareness methods based on psychological theories. *African Journal of Business Management*. Vol 5 (26)
29. Daniel. E (2016). The Usefulness of Qualitative and Quantitative Approaches and Methods in Researching Problem-Solving Ability in Science Education Curriculum. *Journal of education and practice* Vol 7(15).
30. Sethi. S, Kaur.A and Kumar. G (2011). Computer Network Attacks- A study. *International Journal of Computer Science and Mobile Applications*. Vol 2, (11).
31. Rainer.R, Prince. B and Cegielski. C (2012). *Introduction to Information Systems*. 5th ed. John Wiley & Sons. United States of America.
32. Gupta. S, Kumar.A and Bhatnagar. R (2016). The Role of Information Systems in a University Setup. A case Study. *International Journal of Computer Science and Electronic Engineering*. Vol 4 (11).
33. Ma and Liu (2014). The Technology Acceptance Model. *Journal of organizational and end user computing*. Vol 16 (1).
34. Aloul. F (2012). The need for effective information security awareness. *Journal of advances in information and technology*. Vol 3 (3).
35. Acguah. H, Twinn. F and Safiana. O (2016). Information System Threats and Vulnerabilities: Evaluating the Human Factor in Data Protection. Vol 143 (5).
36. Kaur. K, (2016). Information Security of an Organization with a focus on Human perspective. *International Journal of Computer Techniques*. Vol 3 (5).
37. Ping. O & and Fatt. C (2014). Information Security Awareness. *International Conference on Computer, Communication Information and Technology*.
38. Solic. K, Ocevcic. H and Blazevic. D (2015). Survey on Password Quality and Confidentiality.

39. Lawroom (nd). Investing in the Human Firewall: Data security training for employee report.
40. Metalidou. E, Marinagi. C, Trivellas. P, Eberhagen. N, Skourlas and Giannakopoulos (2014). The Human Factor of Information Security. Social and Behavioral Sciences.
41. Rajendran. S and Shenbagaraman. V (2016). A study on Protection Theory and Information Systems Security Police Compliance. International Journal of Pharmaceutical Science Review and Research.
42. Solic. K, Nenadic. K and Galic. D (2012). Empirical Study on The Correlation between User Awareness and Information Security. International Journal of Electrical and Computer Engineering. Vol 3 (2).
43. Hostiad. D and Surdama. M (2016). Implementation of Email Security Using PGP at Zimbramail server. International Journal of Computer. Vol 13 (6).
44. Warkentin. M, Malimage. N and Kalana. M (2012). Impact of Protection Motivation and Deterrence on IS Security Policy Compliance: A multi-Cultural View. Associations for Information Systems.
45. Pfleeger. P (2006). Security in Computing. 4th ed. Prentice Hall.
46. Rainer. R and Harrison. A (1992). The influence on individual difference on skill on End user computing. Journal of management in information systems. Vol 9 (1).
47. Osang. E, Udoimuk. B, Etta. B, Ushie. O and Offiong. E (2013). Methods of Gathering Data for Research Purpose and Applications Using IJSER Acceptance Rate of Monthly Paper Publication. IOSR Journal of Computer Engineering. Vol 15 (2).
48. Boell. S and Keemanovic, D (2015). What is an Information System. Hawaii International Conference on System Sciences.
49. Whitman. M and Mattord. H (2011). Principles of Information Security. 4th ed. Cengage. United States of America.
50. Makau. B and Akaranga. S (2016). Ethical Consideration and their Application in Research. Vol 3 (12).
51. Kulkarni. S (2015). A Survey of Password Attacks, Countermeasures and Comparative Analysis of Secure Authentication Methods. International Journal of Advance Research in Computer Science and Management Studies. Vol 3 (11).

52. Bird. D (2009). The use of questionnaire for acquiring information on public perception of natural hazards and risk mitigation.
53. Wawak. S (2010). The Importance of Information Security Management in Crisis Prevention in the Company. 6th International Symposium on Business Administration.
54. Kamal. P (2019). Security of password hashing in cloud. Journal of Information Security.
55. Singh. S, Singh. M and Singh. D (2011). A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks. International Journal of Computer Trends and Technology: ISSN 2231-2803.
56. Henderson. A (2017). The CIA Triad: Confidentiality Integrity and Availability.
57. Karwowski. W and Glaspie. H (2018). Human Factors in Information Security Culture.
58. Chandel. A, Kumar. P and Yadav. D (2017). Phishing Attack and Its Countermeasures. International Journal of Advanced Research in Computer Science and Software Engineering. Vol 7 (6).
59. Awan. A (2006) Security Risk Analysis
60. Kaabouch. N and Salahdine. F (2019). Social Engineering Attacks.
61. Grant. C and Osanloo. A (2014). Understanding Selecting, and Integrating a Theoretical Framework in Dissertation Research. Vol 4 (2).
62. Hindle. J and Clubb. A (2015). Protection Motivation Theory as a theoretical framework for understanding the use of protective measures. Criminal Justice studies. Routledge Taylor and Francis Group.
63. Organization for Economic Corporation and Development (OECD) (2002). Guidelines for the security of information systems and networks.
64. Kranz.J and Haeussinger. F (2013). Information Security Awareness. Its antecedents and mediating effects on security complaint behavior. Thirty Fourth International Conference on Information Systems.
65. Hash. J and Wilson. M (2003). Building an Information and Technology Awareness and Training Program. NIST-SP 800-50
66. Probst. J and Hunker. C (n.d). Insider and Insider threats an overview of definitions and mitigation techniques.
67. Cilliaris. F (2015). Improving Information Security in SME to protect customer identifiable information.

68. Kranz. J, Kolbe. L and Muntermann. J (2015). Studies on Employee's Information Security Awareness. Thesis University of Gottingen.
69. Denev. T and Hu. Q (2007). The Centrality of Awareness in The Formation of User Behavioral Intentions towards Protective information and Technology. Journal of the Associations for Information Systems. Vol 8 (7).
70. Veiga. A (2015). An Information Security Training and Awareness Approach to instill an Information Security Positive Culture. Proceeding of the Ninth International Symposium on Human Aspects on Information Security and Assurance.
71. Sawahel. W (2017). University face an age of cybercrime. Available at [<https://www.universityworldnews.com/post.php?story=2017092208032052>]. Accessed: 12 September 2019.
72. Chareon. D (2014). Password Security. International Journal of Security. Vol 8 (1)
73. Hadlington (2018). Employee Attitude towards Cybersecurity and Risky Online Behaviors. Vol 12 (1).
74. Mathers. N, Fox. N and Hunn. A (2009). Surveys and questionnaire. National Institute for Research.
75. Hinson. G (2003). Human Factors in Information Security. Innovative Information security awareness program white paper.
76. Greitzer. F and Hohimer. R (2011). Modeling Human Behavior to Anticipate Insider Attacks. Journal of Strategic Security. Vol 4 (2).
77. Kaur. M (2017). Data Encryption Using Different Techniques. International Journal of advanced Research in Computer Science. Vol 8 (4).
78. Rose.M (2016). Physical security.
79. Walters. P (2012). The Risks of Using Portable Device. United States of Computer Emergency Readiness Team (US-CERT).
80. Suhail,Q and Quadri. S (2016). Information Availability: An insight into Most Important Attribute of Information Security. Journal of Information Security. Vol 7.

APPENDIX

Appendix A Questionnaire

Please Tick ✓

1. What is your Gender?

Male ☐ Female ☐

2. What is your Age?

21-30 ☐ 31-40 ☐ 41-50 ☐ 51 and above ☐

3. What is your educational Background?

Primary Education ☐

Secondary Education ☐

Higher Education ☐

Post Graduate/Doctorate ☐

4. What is your Field of study?

ICT ☐ Non ICT ☐

5. What is your position in the organization?

Lecturer ☐ Administrative officer ☐

General threats to Information Systems

6. Rate your understanding about threats to information security?

Very Moderately ☐ Moderate ☐ Slightly ☐

7. Rate your knowledge on the following types of threats to information security?

High ☐ Medium ☐ Low ☐

Social Engineering
Brute force attack
Denial of service
Phishing
Spam attack
Ransomware
Dictionary attack
Data breach
Information leakage
Cyber espionage
Cyber terrorism

8. Whom do you feel should take measures to stop the spread of computer virus, fraudulent mail, spyware and spam?

Internet Service Provider (ISP) ☐

Antivirus software companies ☐

Computer software companies ☐

System administrators ☐

Technical control

9. Do you know the type of antivirus installed into your computer?

Yes ☐ No ☐

10. Do you scan your memory stick before opening it?

Yes ☐ No ☐

11. What action would you take when you encounter a pop notifications that you must restart your computer to install important updates?

Restart the computer ☐

Ask for help ☐

12. How do you react to Email links recommended to you by employees who left the company?

Confirm details before clicking ☐

Click details without confirming ☐

Ignore ☐

13. How do you react when you notice that the contents of your inbox has been deleted?

Restart the computer ☐

Report immediately ☐

Observe the situation ☐

Log into another computer ☐

14. Do you always confirm if the website you access is secure?

Yes ☐ No ☐

15. Have you ever forwarded an email to your work mate suspected to be spam?

Yes ☐ No ☐ Maybe ☐

16. Have you ever opened an email attachment from unknown source?

Yes ☐ No ☐ maybe ☐

17. Do you encrypt confidential information before sending it over the internet?

Yes ☐ No ☐

Password management

18. Do you log into your computer at work using a password or username?

Yes ☐ No ☐

19. Have you ever shared your password to someone?

Yes ☐ No ☐

20. How do you secure your password?

Note it on paper ☐ Memorize it ☐ Save in cell phone ☐

21. Do you change your password after some interval of time?

Yes ☐

No ☐

22. Do you use the same password to log into different computers or applications?

Yes ☐ No ☐

23. What is the minimum length for your password?

4 characters ☐

5 characters ☐

8 characters ☐

14 characters ☐

24. Is your password a combination of symbols, numbers and characters?

Yes ☐ No ☐

Physical security

25. Do you log out on your computer open when you are called for a meeting?

Yes ☐ No ☐

26. Do you switch off your computer after working hours?

Yes ☐ No ☐

27. Is security camera more important than a guard man?

Yes ☐ No ☐

28. Rate you level of knowledge on the use of fire extinguisher in case of emergency?

Very High ☐ High ☐ Medium ☐ Low ☐

Thoughts on Organizational policy

29. Do you think establishing policy to restrict file downloads and using of removable drives like USB is important?

Strongly Agree ☐ Disagree ☐ Strongly Agree ☐

30. Do you agree that too much file downloads at work is risky to information security?

Yes ☐ No ☐ Maybe ☐

31. Do you backup your data?

Yes ☐ No ☐

32. Have you ever participated in security awareness programs?

Yes ☐ No ☐

33. Are you are aware of information security policy in your institution?

Yes ☐ No ☐

B. Questions Code Microsoft office Excel

1	ID	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16
2	1	1	2	3	2	2	3	3	2	2	2	1	2	2	2	3	
3	2	2	2	3	2	2	3	3	4	2	1	1	1	2	1	3	
4	3	2	3	3	2	2	3	3	3	2	2	1	2	2	1	1	
5	4	1	3	4	2	1	1	2	3	2	2	1	2	2	1	1	
6	5	2	2	3	2	2	3	3	4	2	1	1	2	2	2	3	
7	6	2	2	4	1	1	1	1	4	1	1	1	2	2	2	3	
8	7	2	2	4	2	1	2	2	2	2	1	1	2	2	2	3	
9	8	2	1	3	2	1	2	3	2	2	1	2	2	1	2	2	
10	9	2	2	4	1	1	1	2	1	1	1	1	1	3	2	2	
11	10	1	4	3	2	1	2	2	2	2	1	1	1	2	2	2	
12	11	1	2	3	1	1	1	3	4	1	2	2	2	1	2	3	
13	12	2	2	3	2	2	1	1	4	2	1	2	1	3	1	2	
14	13	1	3	4	2	1	3	3	3	2	2	2	2	4	2	1	
15	14	1	3	4	2	1	2	2	3	2	2	2	2	1	2	1	
16	15	2	3	3	2	1	2	3	4	2	2	2	2	4	2	1	
17	16	2	2	4	2	1	1	3	2	2	2	1	2	4	2	3	
18	17	2	2	4	2	1	1	1	2	2	1	1	2	3	2	3	
19	18	2	1	3	2	1	2	2	2	2	1	1	2	4	2	2	
20	19	2	1	4	1	1	2	2	4	2	1	1	1	3	2	2	
21	20	1	2	4	2	1	3	3	2	2	1	1	1	2	1	2	
22	21	1	2	3	1	1	2	2	4	1	1	1	1	2	2	2	
23	22	2	2	3	1	1	1	1	4	1	1	1	1	2	2	2	
24	23	1	4	4	2	1	1	3	3	2	1	1	2	2	2	1	
25	24	2	1	4	2	1	2	3	3	2	1	1	2	2	1	1	
26	25	2	2	4	2	1	2	3	4	2	1	2	2	1	1	1	
27	26	2	2	4	2	1	1	2	2	2	1	2	2	2	2	3	
28	27	2	2	4	2	1	3	3	2	2	1	1	2	4	2	3	
29	28	2	1	3	2	2	2	1	2	2	1	2	2	2	1	2	
30	29	1	2	3	2	2	2	3	1	2	1	1	1	3	1	2	
31	30	1	4	4	2	1	3	2	2	2	2	1	1	2	2	2	
32	31	2	1	3	2	2	1	3	4	2	1	1	1	3	2	1	
33	32	2	2	4	2	2	2	3	4	2	1	2	1	3	2	1	
1	Q16	Q17	Q18	Q19	Q20	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30	Q31	Q32
2	1	2	1	2	2	1	2	1	1	1	2	1	3	2	3	2	
3	1	2	1	1	1	2	1	3	1	1	2	1	3	2	2	2	
4	1	1	2	2	2	1	1	3	2	1	1	1	4	2	2	2	
5	1	1	2	2	3	2	2	3	2	1	2	1	4	2	2	2	
6	1	1	2	1	2	1	1	1	2	1	1	2	3	1	3	2	
7	1	2	1	1	3	1	1	3	1	1	2	1	4	1	1	1	
8	1	2	1	2	2	2	1	2	1	1	2	1	3	1	1	1	
9	3	2	1	1	3	1	2	4	1	1	1	2	4	1	3	2	
10	1	2	1	1	2	1	1	2	1	1	1	1	3	1	1	1	
11	1	2	1	2	2	1	1	4	1	1	2	1	4	3	3	1	
12	1	2	1	1	2	2	1	4	1	1	2	1	4	1	1	1	
13	3	2	1	1	1	1	1	3	1	1	2	1	4	2	2	2	
14	1	2	2	2	2	2	1	2	3	2	1	1	4	2	2	2	
15	1	2	2	1	2	2	2	1	3	2	1	2	1	3	2	2	
16	1	2	2	1	1	1	1	1	2	1	1	2	3	3	3	2	
17	1	2	1	2	3	2	1	2	1	1	2	1	3	3	3	1	
18	1	2	1	1	2	1	1	3	2	2	2	1	4	3	3	1	
19	3	2	1	2	2	2	1	3	2	2	1	2	4	1	2	2	
20	1	2	1	1	2	1	1	4	1	1	1	1	4	1	1	2	
21	1	2	1	2	3	2	1	3	1	1	1	1	3	3	3	1	
22	1	2	1	1	2	1	1	4	1	2	2	1	4	1	2	1	
23	1	1	1	1	1	2	2	3	1	2	2	1	4	2	2	2	
24	1	2	2	1	2	1	2	3	2	1	1	1	4	2	2	2	
25	1	2	2	2	2	2	2	3	2	1	1	2	4	2	2	2	
26	1	2	2	1	3	1	1	4	2	2	1	1	4	2	3	2	
27	1	2	1	2	2	1	1	3	1	2	2	1	4	2	3	1	
28	1	2	1	1	2	1	1	3	1	2	2	1	3	2	3	1	
29	3	2	1	2	3	2	2	3	1	2	2	2	3	2	3	2	
30	1	2	1	1	2	1	1	3	1	1	2	1	4	1	2	1	
31	1	2	1	2	2	1	1	4	1	1	1	1	3	3	3	1	
32	3	2	2	1	1	2	2	1	2	2	2	1	4	2	2	1	
33	1	2	2	1	2	2	1	4	2	2	2	1	4	2	2	2	
1	Q32	Q33	Q34	Q35	Q36	Q37	Q38	Q39	Q40	Q41	Q42	Q43	Q44	Q45	Q46	Q47	Q48
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	
3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	
4	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	
5	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	
6	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	
7	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	
8	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	
9	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	
10	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	
11	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	
12	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	
13	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	
14	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	
15	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	
16	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	
17	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	
18	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	

C. Consent form to take part in research study

Research Title

Investigation on The Level of Information Security Awareness Among employees

I..... voluntarily agree to participate in this research study.

I understand that even if I agree to participate now, I can withdraw at any time or refuse to answer any question without any consequences of any kind.

I understand that participation involves responding to the questionnaire that shall be availed to me by the researcher.

I understand that I will not benefit directly from participating in this research

I understand that all information I provide for this study will be treated confidentially and will be used for the research study only

I understand that in any report on the results of this research my identity will remain anonymous. This will be done by changing my name and disguising any details of my interview which may reveal my identity or the identity of people I speak about.

I understand that signed consent forms will be securely stored until the exam board confirms the results of the dissertation.

I understand that under freedom of information legalization I am entitled to access the information I have provided at any time. I understand that I am free to contact any of the participants involved in the research to seek further clarification and information.

Signature of participant _____

Email address: _____

I believe the participant is giving informed consent to participate in this study

Signature of researcher _____

Date _____

Appendix D Phishing web form

A PLATFORM FOR SUCCESFULL LECTURES FILL IN YOUR DETAILS TO RECEIVE WEEKLY UPDATES OB BEST LECTURING METHODS [Click the link to access articles for professional lecture](#)

Name:

Gender: ☒ Male ☐ Female

Email :

Contact No: +267

HTML Code:

```
<!DOCTYPE html>
<html>
<head>
<title>
Free lecture article
</title>
</head>
<body>

<body bgcolor="orange"
<h1>
A PLATFORM FOR SUCCESFULL LECTURES FILL IN YOUR DETAILS TO RECEIVE WEEKLY UPDATES OB BEST LECTURING METHODS
</h1>
<a href="http://thimhaingura@gmail.com">

Click the link to access articles for professional lectures
</a>
<form>
  <table>
    <tr>
      <td>
Name:
      </td>
      <td>
<input type="text" placeholder="Name" name="">
      </td>
    </tr>
    <tr>
      <td>
Gender:
      </td>
      <td>
<input type="radio" name="Gender">Male
<input type="radio" name="Gender">Female
      </td>
    </tr>
  </table>
</form>
</body>
</html>
```

```

</td>
</tr>
<tr>
<td>
Email :
</td>
<td>
<input type="mail"placeholder="Email" name="">
</td>
</tr>
<tr>
<td>
Contact No:
</td>
<td>
<select>
<option> +267</option>
<option> +264</option>
<option> +27</option>
</select>
<input type="Phone" placeholder="+267*****" name="">
</td>
</tr>
<tr>
<td>
<input type="Submit" value="Submit" name="">
</td>
</tr>
</table>
</form>
</body>
</html>

</table>
</form>
</body>
</html>
<td>

```