INFORMATION SECURITY ADHERENCE IN INSTITUTIONS OF HIGHER EDUCATION: A Case Study of American University of Nigeria

ODEGBESAN OMOBOLAJI AYOMIDE

A00018467

In partial fulfillment of the requirement for the award of degree of Master of Science (MSC) in Information Systems submitted to
The School of Graduate Studies (SGS), American University of Nigeria.

Fall 2017
CERTIFICATION

I certify that the work in this document has not been previously submitted for a degree nor has it been submitted as a part of a requirement for a degree except fully acknowledged within this text.

----------------------------
Odegbesan Omobolaji Ayomide
Student

----------------------------
---------------------------------
Dr. Salihu Dasuki
Supervisor
Dr. Charles Nche
Supervisor

----------------------------
Dr. Mathias Mbu Fonkam
Dean SITC
DECLARATION

I, ODEGBESAN OMOBOLAJI AYOMIDE, declare that the work presented in this thesis entitled ‘INFORMATION SECURITY ADHERENCE IN INSTITUTIONS OF HIGHER EDUCATION: A Case Study of American University of Nigeria’ submitted to the School of Graduate Studies, American University of Nigeria, in partial fulfillment for the award of the Master of Science (M.Sc.) in INFORMATION SYSTEMS. I have neither plagiarized nor submitted the same work for the award of any other degree. In case this undertaking is found incorrect, my degree may be withdrawn unconditionally by the University.

Date: December 2017
Name: Odegbesan Omobolaji Ayomide

Place: Adamawa Yola, Nigeria
ID.No: A00018467
ACKNOWLEDGEMENT

All thanks to God, the Almighty, He that giveth and taketh. I thank him for being with me till this day and for seeing me through to this point in my academic programme.

My profound gratitude goes to Dr. Salihu Dasuki and Dr. Charles Nche for been such supportive supervisors. Both have been very consistent in providing me with guidance, and endless counselling and mentoring support. I am also thankful to Dr. Ago Quaye, Dr. Chidi Ononihu, Dr. Mathias Mbu Fonkam and Dr. Rajesh Prasad for their encouragement, support and assistance. I am also appreciative of their unlimited support in improving my research skills. Many thanks for their patience, effort and valuable guidance.

I am very grateful to my parents for their unlimited support, guidance and assistance throughout my academic programme. For without them none of this would ever have been possible. I also wish to say a big thank you to my Uncle for his love and support.

Last but not the least, I wish to express my deepest gratitude to everyone that have contributed directly or indirectly to the successful completion of this thesis.
Abstract

Institution of higher education face a higher level of information security incidence and compromise such as data and information theft, malicious program infection, attack on the information systems infrastructure and computer network. The antagonistic impact of information security incidence includes compromise of confidential data and intellectual property, massive financial losses and increased level of information security vulnerability and threat. This study aims to determine the predictors of students’ adherence to safe information security behaviour in institution of higher education. In this study, we integrate variables from the Protection motivation theory (PMT) and the Unified theory of acceptance and use of technology (UTAUT) theory in other to understand the willingness of student to practice safe information security behavior. This study utilized the quantitative research method for data gathering and analysis. A total of 276 responses where gotten from the respondents. The result showed that the threat appraisal, performance expectancy, effort Expectancy have significant impact on the intention to adhere to a safe information security behavior. While facilitating condition have significant impact on actual protection and also the intention have a significant impact on actual information security behavior. From the research findings, we identified threat appraisal, performance expectancy, effort expectancy, facilitating condition as the different predictors of student adherence to safe information systems security behavior. The research findings suggest that safe information security behavior is influenced by information security education and awareness. Furthermore adequate support also influence safe information security behavior.
Table of Contents

ACKNOWLEDGEMENT ........................................................................................................ iv

Abstract ................................................................................................................................ v

List of Table ........................................................................................................................... Error! Bookmark not defined.

List of Figure ........................................................................................................................ Error! Bookmark not defined.

CHAPTER ONE .................................................................................................................... 1

INTRODUCTION .................................................................................................................. 1

1.0 BACKGROUND TO THE STUDY .................................................................................... 1

1.1 STATEMENT OF PROBLEM ............................................................................................ 4

1.2 OBJECTIVE OF STUDY .................................................................................................... 5

1.3 RESEARCH QUESTION ...................................................................................................... 5

1.4 SCOPE OF STUDY ............................................................................................................ 6

1.5 PLAN OF THE STUDY ....................................................................................................... 6

CHAPTER TWO ....................................................................................................................... 8

LITERATURE REVIEW ............................................................................................................ 8

2.0 INTRODUCTION ............................................................................................................... 8

2.1 INFORMATION SYSTEMS IN INSTITUTIONS ................................................................... 8

2.2 INFORMATION SECURITY IN INSTITUTIONS ................................................................. 12

2.3 CHARACTERISTICS OF INFORMATION SECURITY ....................................................... 14

2.4 INFORMATION SECURITY THREATS AND ATTACKS IN INSTITUTIONS OF HIGHER EDUCATION ........................................................................................................ 15

2.4.1 KEYBOARD CAPTURING ............................................................................................. 15

2.4.2 MALWARE .................................................................................................................... 16

2.4.3 DENIAL OF SERVICE ATTACK ..................................................................................... 16

2.4.4 SNIFFER ....................................................................................................................... 17

2.4.5 FILE SHARING THREATS ........................................................................................... 18

2.4.6 EXCESS AND ABUNDANCE OF INTERNET RESOURCE ............................................. 18

2.4.7 INSTANT MESSAGE TECHNOLOGIES ......................................................................... 19

2.5 THEORETICAL BACKGROUND ...................................................................................... 19

2.5.1 THE PROTECTION MOTIVATION THEORY (PMT) ................................................... 21

2.5.2 THE UNIFIED THEORY OF ACCEPTANCE AND USE OF TECHNOLOGY (UTAUT) ... 24

2.6 RESEARCH HYPOTHESIS ............................................................................................... 26

2.6.1 THREAT APPRAISAL ................................................................................................. 27
2.6.2 PERFORMANCE EXPECTANCY .............................................................. 28
2.6.3 EFFORT EXPECTANCY .................................................................. 28
2.6.4 FACILITATING CONDITION ......................................................... 29
2.6.5 INTENTION .................................................................................. 29
2.7 CHAPTER SUMMARY ..................................................................... 30
CHAPTER THREE .......................................................... 31
RESEARCH METHODOLOGY ................................................. 31
3.0 INTRODUCTION ............................................................................ 31
3.1 RESEARCH DESIGN ................................................................. 31
3.2 POPULATION OF THE STUDY ..................................................... 32
3.3 POPULATION AND SAMPLING ..................................................... 32
3.4 METHOD OF DATA COLLECTION .................................................. 33
3.5 RESEARCH INSTRUMENT ........................................................... 34
3.6 RESEARCH INSTRUMENT VALIDITY AND RELIABILITY .............. 34
3.7 ADMINISTRATION OF RESEARCH INSTRUMENT ..................... 35
3.8 ETHICAL CONSIDERATIONS ......................................................... 35
3.9 METHOD OF DATA ANALYSIS ....................................................... 35
CHAPTER FOUR .............................................................. 37
DATA ANALYSIS AND FINDING .............................................. 37
4.0 INTRODUCTION ............................................................................ 37
4.1 DEMOGRAPHIC CHARACTERISTICS OF RESPONDENTS ............ 37
4.2 DATA ANALYSIS .......................................................................... 38
4.3 COMMON METHOD VARIANCE ANALYSIS ................................. 39
4.4 EXPLORATORY FACTOR ANALYSIS TESTING ......................... 39
4.4.1 RELIABILITY AND VALIDITY ................................................... 40
4.5 CONFIRMATORY FACTOR ANALYSIS ........................................ 40
4.5.1 THE RELIABILITY AND CONSTRUCT VALIDITY MEASUREMENT 40
4.5.2 MODEL FIT ............................................................................. 42
4.6 HYPOTHESIS TESTING ............................................................... 43
CHAPTER FIVE .............................................................. 45
DISCUSSION AND CONCLUSION ........................................... 45
5.0 DISCUSSION ................................................................................. 45
5.1 THREAT APPRAISAL ................................................................. 46
5.1.1 PERFORMANCE EXPECTANCY ..................................................................................... 46
5.1.2 EFFORT EXPECTANCY .......................................................................................... 47
5.1.3 FACILITATING CONDITION ................................................................................ 47
5.2 IMPLICATION ............................................................................................................. 48
5.3 LIMITATION ............................................................................................................... 49
5.4 SUGGESTION FOR STUDY ...................................................................................... 49
5.5 CONCLUSION ............................................................................................................ 50
REFERENCE ................................................................................................................... 51
APPENDICES ................................................................................................................ 61
APPENDIX 1: SURVEY QUESTION .................................................................................. 61
    Questionnaire ................................................................................................................ 61
    Informed Consent ......................................................................................................... 61
    Demographic ............................................................................................................... 63
    Threat Appraisal ........................................................................................................ 63
    Performance Expectancy ............................................................................................ 63
    Effort Expectancy ....................................................................................................... 64
    Facilitating Condition ................................................................................................ 65
    Intention ...................................................................................................................... 65
    Actual Behavior .......................................................................................................... 66
APPENDIX 2: PATTERN MATRIX .................................................................................. 67
APPENDIX 3: COMMON METHOD VARIANCE TEST ..................................................... 68
APPENDIX 4: KMO AND BARTLETT’S TEST AND TOTAL VARIANCE EXPLAINED ...... 69
CHAPTER ONE
INTRODUCTION

1.0 BACKGROUND TO THE STUDY

Information is an essential resource and asset; the possession of relevant, correct and detailed information has increased institutional and organizational effectiveness and efficiency. Modern technologies and innovations, have transformed how data are collected, processed and disseminated. However the availability and ease of access to modern information technologies and innovation have led to unauthorized and improper collection, sharing, modification, exchange and dissemination of information and data (Varney, 1996); due to this, information protection and security has become a critical issue. The need for the protection of information and its assets have become paramount in institutions and organization (Marks, 2007). However, institutions and organization must ensure that proper information security practice become a common practice in their regular and daily processes and activities.

Information security is the adequate protection of information and its essential assets against unauthorized access, modification and misuse by individuals, group of people and organization (Whitman & Mattord, 2011). The main objective of information security in institutions includes the prevention, avoidance, detection, and recovery of information and its essential asset (Awad & Battah, 2011).

Information security is not limited to the protection of information and data alone, it also ensures the protection of the entire information infrastructure and assets (Okibo & Ochiche, 2014). Information security cut across hardware, software, threats and challenges, physical security and also the human behavior. However, there is need to understand every aspect of information
security in order to proffer effective and efficient information security measure and procedure for adequate protection of information and its assets. Furthermore, the increase accessibility to information and its asset have led to a high susceptibility level to threats, and attacks. Also high vulnerability to threat, and attack have made the tightening of information security a major priority in organizations and institution (Al-awadi & Renaud, 2007; Seely & Duguid, 2000).

The security attainment and the utilization of technology is not sufficient enough to ensure adequate information security; consideration has to be given to the organization and institution itself (Segev, Porra, & Roldan, 1998). In other to strengthen Information security there should be increased deliberation on both technical and non-technical aspect. Furthermore, information security implementation in institutions should cover both human and ethical prospect and consideration (Trompeter & Eloff, 2001).

Harrell, (2014) stated that insider threats expose the information security of institutions to threat, attack and vulnerabilities and this as a momentous and significant effect on both the institution and the organization as a whole. The 2013 & 2014 United States of cyber-crime review and study Carnegie Mellon CERT Program showed that those who have legitimate access to the organizations and institutions information systems pose a high level of threat to the institutional information system asset and infrastructure. It was further stated that insiders are more likely to pose a high level threat, risk, and danger to the information system of the organization than the external users such as hackers and/or other remote (CERT, 2014; Pwc, 2013).

For several decades, information security and confidentiality in institution of higher education have been a major concern (Marks, 2007; Okibo & Ochiche, 2014). The institution of higher education have been a victim and target to information security compromise and cyber-attack for two major reasons (Katz, 2005): First, this is due to the vast amount of computing power that they
have; Secondly because of the open access they provide to the public and their environment. The information systems infrastructure in institution of higher education are not only designed to serve the needs of staffs, student and faculty alone but also to serve and accommodation the needs of guests and researchers. While the nature of higher educational institution involve openness and transparency to the public and a constant distribution of information, a balance must be maintained in other to ensure that information assets are not been exposed to risk or compromised (Smith, 2013).

A breach in a universities’ information asset can undermine its integrity and growth. In the context of higher educational institution, there is a need to properly understand Information security threats and challenges facing higher educational institutions in other to prevent potential loss of information and knowledge assets (Marks, 2007).

In this study, we would be investigating and examining the predictors of student adherence to safe Information security behavior in the institution of higher education. Most literatures on information security in institution of higher education are technical in nature with little consideration on institutional and individual issues and behavior (Mahabi, 2010). Many institutions do not pay attention to the individual behavior and value of information security. However, high level of priority is given to the technical aspect of information security. Due to the high level of technical failure caused by human error, institutions of higher education needs to be aware of the necessity of understanding the institutional and individual behavior and issues alongside the technical facet of information security (Marks, 2007). The technical and non-technical facet of information security should be balanced while continuous improvement and learning is ensured (Rezgui & Marks, 2008).
In this study, American university of Nigeria (AUN) has been chosen as a case study. The American University of Nigeria is among several number institutions with growing amount of delicate and critical data. Interconnectivity amongst the university stakeholders is increasingly required in order to remain competitive and functional in the global economy, but every connection increases the vulnerability level of the institution to threats and attacks.

1.1 STATEMENT OF PROBLEM

The increased use of information capital in institution of higher education have led to the increase level of information security incidence and compromise in institution of higher education (Rezgui & Marks, 2008). There is high reliance on information capital in institution of higher education (Okibo & Ochiche, 2014). Coleman & Purcell (2015) stated that the institutions of higher education are exposed to high level of data and information security breach and compromise.

In institutions of higher education, there is a problem of inadequate implementation of information security, this has led to the various information security compromise and financial loss (Marks, 2007; Rezgui & Marks, 2008). The utilization of only technical approach for the implementation of information security is insufficient (Ifinedo, 2014). Studies have shown that for adequate and effective information security to be ensured, consideration has to be given to both technical and non-technical facet of information security (Brown, 2017). Little consideration is given to institutional and individual issues and behavior (Klein & Luciano, 2016; Mahabi, 2010).

Previous studies have shown that institutions of higher education in Nigeria are vulnerable to information security incidence and compromise. The improper information security behavior of student in institution of higher education leads to data and information compromise of both the student and the institution as a whole (Sodiya A.S, 2004).
An examination of behavioral intention to information security by student’s institution of higher education could result to the proper implementation of information security policy, procedure and mechanism. Furthermore, this could encourage decisive social change in information security and also contribute to securing institution of higher education information systems infrastructure.

1.2 OBJECTIVE OF STUDY

This study aims to examine the predictors of student adherence to safe information security practice in institution of higher education in Nigeria using American University of Nigeria as a case study. The specific objectives of the study include:

- To examine the willingness of student’s adherence to safe information security behavior in American university of Nigeria.
- To examine the predictors that affect student adherence to safe information security practice in American university of Nigeria.
- To examine the student’s information security behavior in American university of Nigeria

1.3 RESEARCH QUESTION

- What are the predictors of student adherence to safe information security behavior in institution of higher education in Nigeria using American University of Nigeria?
- To what extent do student preform safe information security behavior in American university of Nigeria?
1.4 SCOPE OF STUDY

This study is limited to identifying the predictor of student adherence to safe information security behavior and the extent to which student are willing to carry out safe information security behavior in American University of Nigeria. The study sought to focus on all categories of students of the institution irrespective of their programme, sex or age.

1.5 PLAN OF THE STUDY

This study is organized into five chapters which are below:

Chapter one deals with the introduction of the study beginning with background to the study, aim and objectives of the study, research questions, scope and definition of terms.

Chapter Two examines the information systems security in institution especially that of the higher educational sector. It also discusses information security in organization and the influential factors that influence the information security behavior. Furthermore, this section discusses the information security threats and vulnerabilities which institutions of higher education are exposed to. Additionally, this section describes the theoretical framework used in this study and the hypothesis of the study.

Chapter Three consists of the method employed in carrying out the study including population, sample and sampling technique, research instrument, method of data collection and method of data analysis.

Chapter Four comprises of analysis of the data collected in chapter three, findings, and discussions of findings and summary of findings.
Chapter Five includes the conclusions of the study, implication of the study for user behaviour and information technology and systems security and recommendations for security conscious information utilisation behaviours.

1.6 Definition of Terms

**Information:** This is a useful set of fresh data or processed data needed by a user in performing a specific task, or achieving a specific purpose, usually obtained over an electronic information system.

**Information security:** This refers to the state of an information source or infrastructure being protected against the unauthorized use of information, especially electronic data, or the measures taken to achieve this.

**Adherence:** This is the personal commitment of an information system user to protection of information, information source or infrastructure against the unauthorized use of information especially electronic data.

**Behaviour:** This refers to the way in which an information system user acts or conducts himself in the use of information over an information system, device or infrastructure.

**Higher education:** This refers to the post-secondary level of education usually at college, university or polytechnic.
CHAPTER TWO

LITERATURE REVIEW

2.0 INTRODUCTION

This chapter provides a comprehensive review of literatures on the subject of information security behaviours of users with the aim of undertaking a deep evaluation of previous views on the subject matter. A review of existing theories bordering on information security behaviour in respect of literature was conducted. Additionally, the review also covers how the emergence, growth and improvement of information system and information communication technology (ICT) has influenced information security behavior in various institutions. Theories such as Protection motivation theory (PMT) and Unified theory of acceptance and use of technology (UTAUT) are discussed.

2.1 INFORMATION SYSTEMS IN INSTITUTIONS

In the last couple of decades, the impact of innovation and technology have been immensely felt in every institutional sector. The influence, growth, and utilization of information systems is not restricted to any one sector (Awad & Battah, 2011). Several institutional sectors share similar part of this technology with minimal difference (Awad & Battah, 2011).

The growth and advancement of information systems has immensely influenced and changed the manner by which institutions carry out their various activities and processes; this has led to the increased effectiveness and efficiency of most institutions. The advancement of information systems and its assets have also influenced the higher educational institutions (Yusuf, Oluwole, & Loto, 2013).
Institutions of higher education are institutions where accumulation and distribution of information are being carried out. The institution of higher education is an intellectual environment where knowledge and information are transferred and circulated (Sagitova, 2012).

In a higher educational environment there is a tradition of a free exchange of idea, knowledge, and information amongst the stakeholders and individuals (Roberts, 2005).

A university utilizes the exchange process mechanism that’s been processed by the market model (Frackmann, 2007). A market model contains different types of mechanisms which are used in determining the reaction and effect of different types of forces which can affect the overall performance of the market (WebFinance, 2015).

The university belongs to the educational sector which provides service to its client. It is a service provider while its major clients are the students. In the university setting there are 3 identifiable flow of information in the exchange process (Frackmann, 2007). The flow of information in higher educational institution includes:

- Circulated information before service is provided. This type of information is known as Ex-ante information:
  - The Potential service receiver is informed by the service provider about the service i.e. the relevant information about the programme that’s to be studied, the information about the design and the shape of the service that’s been provided. In this instance, it’s the curriculum according to the need (of the labour and society market) (Frackmann, 2007).
  - Information about the institution might be provided for the service received (Frackmann, 2007)
• Information that follows the service which is to be provided by the service provider. This type of service is known as accompanying information.
  ▪ The educational system involves the transfer of information. The accompanying information includes the contact information and other information such as application, enrollment, course and exam registration, student records, user manual, curriculum (Frackmann, 2007).

• Information that is provided after the provision of service. This type of information is known as the Ex post information.
  ▪ A service evaluation might be done by both the service provider and the service receiver (Frackmann, 2007).

![Figure 1 - The University exchange process model (Frackmann, 2007).](image)

In the contemporary institution of higher education, information is an essential part of the university and management process since the entire institution existence is based on its production, transfer, and consumption. Also information forms foundation for the effective and efficient
functioning of every aspect of the institution. Furthermore the appropriate and sufficient usage of information flow in many trends ascertains the outcome of the modern institution activities and process (Frackmann, 2007). Information collected, gathered and used in the institution of higher education have to be exhibited and organized in an intelligent and consistent manner. This information has to be adequately managed and maintained for its proper dissemination and usage. Information systems are used to properly, effectively and efficiently manage and maintain information in every institutional sector as well as universities and other educational institutions (Frackmann, 2007).

Information systems can be defined as the unified array of component that are used for the collection, storage and processing of data for the provision of information, knowledge and also digital product. It is the application of interdependent and collective network that institutions and individuals use to collect, gather, filter, process, create and distribute data (Awad & Battah, 2011; Sagitova, 2012; Zwass, 2016).

Information system is an essential part of the universities processes and activities. It aids and support resources and information flow in the higher educational institution; it also aids users to adequately, effectively and efficiently work in environment where facts, data, are to be processed, managed and computed. Furthermore, information systems aids individuals to adequately perform their required and relevant functions. A university institutional information system is a technical and departmental system where IT system are utilized and realized; both the hardware and software are utilized for the collection, gathering, processing, acquisition, storage, search and dissemination of data and processed information (Sagitova, 2012).

The higher educational institutions (universities) information system is complex when compared to other institutional sectors information system. Its complexity does not prevent or deter it from
catering for the demands of its stakeholders and the institution in general (Luo & Warkentin, 2004). The higher educational institution is an environment which contains individuals with high intellect, these individuals have the freedom and motivation to explore the cutting edge technologies in the institution and can lead to the compromise of the university’s information system. Additionally, the conventional practice in a university environment is one which aids, promotes and encourages the free exchange of ideas and knowledge (Sagitova, 2012). The instant access to the Information systems educational tools benefits the academic mission and goals of the university. Due to the access and high dependency on the information systems tool, there is a high risk of information system compromise in a university environment (Roberts, 2005). The compromise of the confidentiality, integrity, and availability (CIA) of the university information has led to the need for information system security (David R. Johnson, Thomas P. Olson, 1989; Sodiya A.S et al., 2004).

2.2 INFORMATION SECURITY IN INSTITUTIONS

Security is the quality and the state of being secured. It is also a state of being generally free of danger or harm (Whitman & Mattord, 2011). Security can be defined as the protection against harm which can be inflicted by individuals or a group of people either intentionally or unintentionally (Whitman & Mattord, 2011). In every institutional sector, there are several forms of security (Whitman & Mattord, 2011). This types of security include:

- The protection of physical object from misuse and unauthorized access and modification. This type of protection is known as a physical security.
- The protection of individuals or a group of people from harm or danger. This type of protection is known as a personal security.
• The protection of activities and process from disruption or modification. This type of protection is known as an Operational Security.

• The protection of communication technology media, device, content and other related equipment from unauthorized access, modification, and misuse. This type of protection is known as Communication Security

• The protection of networking media, component, equipment connections, and contents. This type of protection is known as network security

• The protection of the confidentiality, integrity, availability of information, assets, it storage, processes or transmission mechanism. This type of protection is known as information security.

In the context of this study; we would be paying attention to information security. Information system security has become a major issue in the higher educational institutions such as the universities. This major concern has led to the increase in the complexity of the information system in higher educational institutions (Awad & Battah, 2011). It was reported by the computer emergency response team (CERT) and other resources that there is a rapid increase in the amount of network intrusion incidence which is as a result of a hacker attacking universities worldwide (Storms, 2004). It was stated that there is a high rate of hackers scanning various universities worldwide for vulnerabilities in their systems; using baits and holding areas like free software, social engineering, free games, digital music and movies to compromise the integrity, confidentiality and availability (CIA) of the systems and to also steal valuable information from the universities and other institutions of higher education information systems (Dunn, 2016).
2.3 CHARACTERISTICS OF INFORMATION SECURITY

Information security means the protection of information and its relevant assets from unauthorized users (Whitman & Mattord, 2011). In other to say an information or an information system is secure, the employed information security must have the following characteristics.

- **CONFIDENTIALITY**
  
  This is the preservation of a system or an information from unauthorized users. A system of an information is said be secure when an unauthorized user does not and can’t have access to the system or information. On the other hand, if an unauthorized individual has access to the system or information then the confidentiality of that system or information is breached or lacking confidentiality (Whitman & Mattord, 2011).

- **INTEGRITY**
  
  This is the preservation of a system or an information from unauthorized modification or change, thereby ensuring the systems or information authenticity and accuracy (Whitman & Mattord, 2011).

- **AVAILABILITY**
  
  This is known as the reliable use and timely access to a system or an information by an authorized user (Whitman & Mattord, 2011).
2.4 INFORMATION SECURITY THREATS AND ATTACKS IN INSTITUTIONS OF HIGHER EDUCATION.

A threat is an incidence that has the ability to trigger harm or cause loss of information (Demchenko, 2010). A threat can be classified into two major categories; External threat and Internal Threat (Hinde, 2002).

The External Threat: These are threats that emanates from outside the university, organization or institution. This type of threat include: Hackers incidence, Computer Virus, Natural disaster and spam email (Al-awadi & Renaud, 2007; Hinde, 2002).

The Internal Threat: These are threats that comes from within the university, institution, firm or organization. This type of threats include: Theft of physical hardware or software, Installation and unauthorized access and use of information system, Human error or mistake (Al-awadi & Renaud, 2007; Hinde, 2002).

In the case of higher educational system there are various types of attack which has been identified by different literatures such as (Ahmad, 2012; Al-awadi & Renaud, 2007; Aloul, Al-ali, Al-dalky, & Al-mardini, 2012; Jouini, Rabai, & Aissa, 2014). In the context of this study, we would be discussing the major attacks identified by the different kinds of literature. The different types of attacks include:

2.4.1 KEYBOARD CAPTURING

This is also known as keylogging or keystroke logging. It is an action in which keyboard struck, activities and information are being recorded or monitored. This type of attack is both an internal and external threat. It can be launched from within the university or institution of higher education.
and also it can be launched remotely through the use of malware and virus. This type attack can be introduced to the information system equipment and devices in other to extract, record and monitor the keyboard information and activities from a systems or a device (Roberts, 2005; Whitman, 2003). This type of process makes use of a software known as key lodger which is used to monitor and record the keyboard activities of a particular system or device. This is a major threat to the information system of a university due to the easy access to the universities information system equipment by different individuals from within and externally (remotely). The universities are easily exposed to this threat because of the easy access to the information system infrastructure of the university by various parties internally and externally (Ahmad, 2012; “Insider Threat Tools | The CERT Division,” n.d.; Loch et al., 1992; Roberts, 2005).

2.4.2 MALWARE

This is software which its main purpose is to disrupt, damage, steal and compromise the integrity, confidentiality, availability (CIA) of an information system. This type of software includes virus, Trojan, warm, keyboard logger e.t.c. This type of attack is both an internal and external threat. This attack can be exacted on the university from within and also it can be exacted remotely through the internet and through an offline installer. This type of program compromise, steals and allow for the control of an information system and its essential asset remotely by an unauthorized user. It grants unauthorized access to individuals by providing them a backdoor into the system (Ahmad, 2012; Loch et al., 1992; Roberts, 2005; Whitman, 2003; Whitman & Mattord, 2016).

2.4.3 DENIAL OF SERVICE ATTACK

The denial of service attack can be an external and internal threat. This is a type of attack whereby an information system and its relevant asset are made unavailable to its intended user temporarily,
indefinitely or permanently (Roberts, 2005). In its attack nature, the host is compromised on the network by contacting a malware, then it converts the infected system to a zombie. This zombie can be easily and remotely controlled which then leads to denial of service attack; whereby the information system resource is made unavailable by flooring (creating a large amount of traffic) the network through the zombie. The zombie is then instructed to send a large amount of traffic to the intended system in order to make it unavailable for its intended use. This type of threat is a major threat to the university and its information system resource due to the vulnerability of the information system resource of universities (Ahmad, 2012; Jouini et al., 2014; Loch et al., 1992; Roberts, 2005; Whitman, 2003; Whitman & Mattord, 2011).

### 2.4.4 SNIFFER

Sniffers are attacks which higher educational institutions information system resource are exposed to both internally and externally. Sniffers are used to compromise the confidentiality, availability, and integrity of information system resource and equipment of a university and other institution. They can be either software and/or hardware which are used by individuals or groups to compromise the integrity, confidentiality, availability information and it relevant assets. These mechanisms are used to capture the digital information that moves through an information system resource and equipment. Sniffers are used to monitor, gather, and capture sensitive information and data such as passwords, credit card details, personal and financial information which can lead to the misuse and identity theft by individuals (Roberts, 2005; Whitman, 2003).

A type of sniffer is a wireless sniffer. These types of sniffers are used to comprise wireless information system resource and equipment. The installation of wireless information system devices used in institutions helps to save financial and human resources; unfortunately, this has also lead to a new security issue and risk. This type of security issues and risk involves the tapping
and sniffing of wireless devices and network which also leads to the theft and compromise of information and data transferred and used within the network by unauthorized users for inappropriate use and purposes (Roberts, 2005; Whitman, 2003). There are various ways to counter this security issue but most of the ways are either expensive, difficult or both to implement and this has led to major threat and risk to institution such as university (Ahmad, 2012; Roberts, 2005; Whitman & Mattord, 2011).

### 2.4.5 FILE SHARING THREATS

The openness and easy exchange of information and data in universities and academic institutional environment has led to a major and dangerous security threat and issues in most institutions if not all. This can lead to a type of threat that exposes the institution to attacks that can be exacted on the university from within and also it can be exacted remotely. This exposes the institution to virus and malware that can easily be introduced to information system equipment and devices (Roberts, 2005; Whitman, 2003). Malware can be downloaded intentionally and unintentionally from the internet and spread due to liberal use of peer-to-peer (P2P) file sharing in most universities, this can undoubtedly lead to the compromise of the computing and information system resource of the universities (David R. Johnson, Thomas P. Olson, 1989; Loch et al., 1992; Roberts, 2005).

### 2.4.6 EXCESS AND ABUNDANCE OF INTERNET RESOURCE

Higher educational institutions acquire a large amount of internet and information system resource such as bandwidth and device. This resources can be used for research and other educational purposes by staffs, faculties, and students; regrettably, this has also lead to an unwanted and dangerous security threat. These resources are been misused by individuals and people within the
higher educational environment which exposes the higher educational institution information system to compromise and unauthorized use and access (Roberts, 2005).

### 2.4.7 INSTANT MESSAGE TECHNOLOGIES

Most of the instant message technologies were initially developed and used for text message and text-based chatting but it has evolved into the internet application suite. Due to this development infected files can be shared over the university network which could undoubtedly comprise the information system of the university and also expose the university information to a major security issue and threat (Loch et al., 1992; Roberts, 2005; Whitman, 2003).

### 2.5 THEORETICAL BACKGROUND

Several theories have been constructed and employed in different and specific cases for different institutional and environmental studies and research.

In this study, a theoretical framework would be developed in order to describe the predictors of student adherence behavior information security adherence behavior. It also illustrates the behavioral intention of student to information security in institution of higher education.

In order to examine the behavioral intention and the predictors of student adherence behavior to information security. This study integrates variables from the protection motivation theory and the Unified theory of acceptance and use of technology (UTAUT) in order to develop a conceptual framework that illustrates student intention towards information security as well as the predictors of adherence behaviour of student towards information security in American university of Nigeria.

The Protection motivation theory has been widely utilized by several literatures in the information security field; this is due to its robust nature which is used for the analysis and exploration of recommended behaviors to prevent the consequences of threats (Willison & Warkentin, 2013).
The protection motivation theory provides a framework to understand the fear appeal and also it explains the individual’s motivation to prevent themselves against information security threats and attacks (Willison & Warkentin, 2013). In other to understand the behavioural intention of student to information security, the Unified theory of acceptance and use of technology (UTAUT) theory was utilized. The Unified theory of acceptance and use of technology (UTAUT) theory is utilized in several literature in order to explain the user intention to accept or perform a behavior or technology (Venkatesh et al., 2003).

Some concepts in the protection motivation theory and the Unified theory of acceptance and use of technology (UTAUT) tend to overlap, we found out that several different terms used in this different theories have related meanings and they overlap each other. For instance Response efficacy of perceived usefulness in the Protection motivation theory is similar to performance expectancy in UTAUT, reflecting the belief that adhering to information security would reduce threats and attack.

The perceived usefulness or response efficacy can be thought of as performance expectancy. The self-efficacy and the response cost in the Protection Motivation theory can be explained by the facilitating condition. (Empirical & Among, 2015; Sun, Wang, Guo, & Peng, 2013).

There is need to understand the various reasons for individual behaviors, acceptance, motivation and performance to information security in an institution of higher educational institution. This behaviors and attitude have to be examined and investigated in various different context and situation. Theories such as (UTAUT), Protection Motivation Theory (PMT), theory of planed behavior (TPB), Theory of reasoned action (TRA) are widely used to explain, examine individual behaviors, acceptance, motivation, and performance of information security. The previously stated theories provide a platform for investigation and examination of individual intention,
attitude, and behavior. In the context of this study we would be utilizing the Unified theory of acceptance and use of technology (UTAUT) and the Protection motivation theory to examine and investigate individual intention, attitude and behavior towards information security.

2.5.1 THE PROTECTION MOTIVATION THEORY (PMT)

This theory provides an explanation for an individual’s protective behavior in a pertinent setting and environment. The fear appeal literature proposed and investigated a number of the motivational model of health behavior. This models include the Protection Motivation theory (PMT), the Health belief model (HBM), Social Cognitive Theory (SCT), The Theory of Reasoned Action (TRA), The Theory of Planned Behaviour (TPB).

All the models were designed to determine variables that point out the various decision that stipulates details and explanations for risk and also in other to estimate and ascertain their ability to anticipate protective attitude and behaviors. Rogers, (1975) stated that handling and coping with threat emergence is derived from processes known as threat appraisal process and coping appraisal process. Several research and literature over the years have identified and classified three main factors for which the motivation for a protective behavior depends upon. This factors include

- The Perceived severity of threat
- The perceived probability of the occurrence or vulnerability
- The efficacy of recommended preventive behavior. Thereafter, the theory was amended by (Rogers, 1983) in Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation, to incorporate perceived self–efficacy which means the confidence level in an individual capability to carry out the prescribed
behavior as a component in the coping appraisal process. The intrinsic and extrinsic benefits of Hardees are risky behaviors

The model also described the Response cost of a protective behavior. In the protection motivation theory (PMT), there are two processes, this processes includes; THREAT APPRAISAL and COPING APPRAISAL (Rogers, 1975), this process serves as interceding variable with an exemplary feature of motive: it provokes, sustains and direct activities. Having a somewhat comprehensive and broad definition, the protection motivation theory (PMT) uses intention as a dependent variable in it model, this was suggested in a study by (Herath & Rao, 2009; Neuwirth, Dunwoody, & Griffin, 2000; Stanley & Maddux, 1986; Steffen, 1990). Attitude and behavior have been pondered and also been thought of as a dependent variable in the protection motivation theory (PMT) (Herath & Rao, 2009); Supplementary to the four main factors of protection motivation theory (PMT), a number of constructs such as anxiety, worry, impediment, Communal factors and socio-demographic variable in allusion to the situation under exploration and investigation.

The protection motivation theory (PMT) was initially seen as been multiplicative in nature and later it was examined as been addictive in nature. Furthermore, (Rogers, 1983) visualized his own model of the protection motivation theory (PMT) has been parallel or an unordered sequence of the appraisal procedure and processes, other models and construct of protection motivation theory (PMT) visualized the processes as sequential and ordered (Herath & Rao, 2009; Tanner, Hunt, & Eppright, 1991).“The Protection Motivation Model: A Normative Model of Fear Appeals”(Tanner et al., 1991) offered postulation of an orderly protection motivation theory (PMT) model which illustrates and identifies that the state of fears concealed by the threat appraisal process, the outcome of threat appraisal is fear, then the protection motivation is invoked as a result of coping appraisal (Herath & Rao, 2009).
The protection motivation theory (PMT) has been utilized in various fields and studies (Herath & Rao, 2009), despite its relation to threats posed to individuals. The PMT is also used to understand an individual action based on their views of threats it poses to them and the environment. Axelrod & Newton (1991), stated that a nuclear threat doesn’t only affect the individual alone but it also affect the surrounding, putting this in the context of information system security, organizational threat doesn’t only affect the organization alone, it also affects the employees within the organization. However, the concepts are used in the fear appeal and the protection motivation literature and constructs which can be used utilized in the information system security context. In the information security literature, the protection motivation theory (PMT) has been utilized in other to identify potential threat and attack which affects organization’s information system security policies, procedure and mechanisms (Pahnila, Siponen, & Mahmood, 2007) and also potential threats and attacks affecting the individual are also added (Herath & Rao, 2009; Woon, Tan, & Low, 2005). The application and utilization of protection motivation theory (PMT) in the context of information system security of an organization, the Protection motivation theory can be used for the identification of threat/attack which poses risk to information system security policies, procedures and mechanism of the organizations compliance situation (Pahnila et al., 2007)
2.5.2 THE UNIFIED THEORY OF ACCEPTANCE AND USE OF TECHNOLOGY (UTAUT)

This is an information system security theory which is based on eight technology acceptance theories/model; the UTAUT is also known as the Unified theory of acceptance and use of technology because it combines and unifies eight different technology acceptance theories/model to form a universal technology acceptance model in the information systems field. The theories for which the Unified theory of acceptance and use of technology (UTAUT) is based on are the Theory of reasoned action (TRA), The Technology Acceptance Model (TAM), The Motivational model, The Theory of Planned Behaviour (TPB), The combined TAM and TPB, The model of personal computer utilization, The Innovation Diffusion Theory and The Social Cognitive Theory (Venkatesh et al., 2003). The Unified theory of acceptance and use of technology (UTAUT) model at its core uses behavioural intention as an indicator of the technology uses behaviour; it explains how the behavioural intention serves as a factor to the technology behavioural use (Thomas, Singh, & Gaffar, 2013; Venkatesh et al., 2003).
The behavioral intention predictors were established on the reviewed eight information system technology adoption model components. The Unified theory of acceptance and use of technology (UTAUT) contains four other constructs in addition to the behavioral intention and use behaviors, this four construct includes.

- Performance Expectancy: This is defined as the degree to which an individual believes that the use of the technology would lead to performance gain (High Performance). This can also be considered as technology perceived usefulness (Venkatesh et al., 2003).
- Effort Expectancy: This can be defined as the degree to which a technology is easy to use and it requires less effort (Venkatesh et al., 2003).
- Social Factor/Influence: This can be defined as the degree to which individuals believe that the important other believe that they should make use of the technology (Venkatesh et al., 2003).
- Facilitating Condition: This is defined as the extent to which technical and organizational infrastructure support is available for the technology use (Venkatesh et al., 2003).

In the Model, there are four moderating variables such as Age, Gender, Education, and Voluntariness of use. In the model, the Performance Expectancy (PE), Effort Expectancy (EE), Social Influence (SI) as a direct impact on behavioral intention and the Facilitating Condition (FC) as a direct impact on the behavioral use. The Impact of the interaction of each of Performance Expectancy (PE), Effort Expectancy (EE), Social Influence (SI) with age and gender (Attuquayefio & Addo, 2014)
2.6 RESEARCH HYPOTHESIS

An individual perspective shows the individual with positive or negative feeling towards stimulus entity (Siponen et al., 2007). Ajzen, (1991), illustrated that intention captures the various motivational features that influence an individuals’ behaviour. It also describes how intensely an individual is eager to attempt to perform a particular behavior that is required of them (Ajzen, 1991b). According to (Venkatesh et al., 2003), the stronger the intention of an individual to perform a behavior or use a technology, the more likely that individual would use a technology or carry out a specific behavior. The stronger the intention of an individual to adhere to a certain information security behavior, the more likely the individual would actually comply with the information system security behavior.
2.6.1 THREAT APPRAISAL

The threat appraisal is a variable in the Protection Motivation Theory (PMT). This variable consists of two dimensions which include; the perceived vulnerability and the perceived severity. Perceived vulnerability is defined as the probability that a negative or undesirable event would occur if no preventive measure is put in place (Boer & Seydel, 1996; Rippetoe & Rogers, 1987). In the context of this study, a negative event is any information security threat or attack. Hence from the perspective of our study, perceived vulnerability refers to a students’ perceived assessment of whether they are vulnerable to information security threat and attack, which will take place if no preventive measure is put in place to tackle them. On the other hand, perceived severity refers to the degree to which both physical and psychological damage which could occur based on the threat and or an attack (Boer & Seydel, 1996; Rippetoe & Rogers, 1987).

In this study, the perceived severity refers to the potential harm/damage which could occur as a result of information security breaches. In the context of our study, we assumed that if student discern that they are confronted with information system security threats and/or attacks (Threat appraisal), also if the students don’t feel that these information system security threats and/or attacks can cause damage/harm to them (Perceived severity), then they will not perform appropriate information system security behavior. Therefore, this made us hypothesize that;

H1: Threat Appraisal affects students’ intention to adhere to safe information security behavior.
2.6.2 PERFORMANCE EXPECTANCY

Performance expectancy illustrates the users' belief of the effectiveness of using the technology. The effectiveness of information security can be illustrated by the degree to which it can help student curtail information security threat, attacks and vulnerabilities. Response efficacy from the Protection Motivation Theory and Performance expectancy are treated as surrogate because they measure the same thing. When individuals consider that adhering to a proper information security behavior would reduce their vulnerability to threats, attack and information security compromise, they would comply to information security with pre-set information security behavior. This decisive relationship can be back by the positive effect of performance expectancy on the behavioural intention in the UTAUT.

We thus propose that

H2: Performance Expectancy affect students’ intention to adhere to safe information security behavior.

2.6.3 EFFORT EXPECTANCY

This is a variable in the UTAUT (Unified theory of acceptance and use of technology) model. It is defined as the degree of ease associated with the use of the system (Venkatesh et al., 2003). The variable within the model is significant in both mandatory and voluntary context usage (Venkatesh et al., 2003). In this study, we expect the Effort Expectancy to be significant and lead to the behavioral intention of the student to adherence a certain information security behavior. It is also expected that the increased levels of ease to adherence to information security will also increase the behavior intention to comply with information system security behavior. Based on this we hypothesized that;
H3: Effort Expectancy affect student intention to adhere to safe information security behavior.

2.6.4 FACILITATING CONDITION
This variable was derived from the UTAUT (Unified theory of acceptance and use of technology) model. This variable was defined by (Venkatesh et al., 2003) as the degree to which a person believes that support exists to help and make the task easy. In other words, the more a resource and opportunity a person believes exist, the easier it is for them to carry out a given task. The sustenance of organization support and technical infrastructure is an essential mechanism for favorable facilitating condition enhancement (Thomas, Singh, & Gaffar, 2013; Venkatesh et al., 2003).

It is presumed that facilitating condition affects actual adherence with information security positively for example if students is exposed to an appropriate facilitating condition; such as adequate time to get acquainted with proper Information security behavior or if they do not have effortless access to information systems security policies and procedure or If the student does not get adequate support on how to perform certain information security procedure, the student would likely not adhere to proper information systems behavior. Hence this leads to the as hypothesizing.

H4: Facilitating condition affects student adherence to safe information systems security behavior.

2.6.5 INTENTION
This is the degree to which individual and a group of people are willing to perform a particular task or action (Ajzen, 1991b). In the context of this study the task is adherence behavior to proper information security practice. In a study carried out by Roger, (1975)”, it was proposed that intention is the most pertinent measure of protection motivation. Several studies on technology acceptance show that intention is a good predictor of actual behavior (Venkatesh et al., 2003) which in the perspective of this study is the adherence behavior to proper information systems
security practice. Furthermore, in this study behavioral intention is an essential index and indicator of the effect of a persuasive information security behavior. This lead to the hypothesis; H5: Student intention to adhere to safe information systems security behavior affects actual information security behavior.

2.7 CHAPTER SUMMARY

This chapter have been able to discuss information systems and information systems security in institution especially that of the higher educational sector. Further this chapter discuss the Information communication technology (ICT), its growth and adoption in institutions and also it also enumerates information systems security, the different threats as well as their effects on organization and institution; the various factor that leads to and causes the threats and attacks that affects the institutions. This chapter concluded by discussing the various theoretical framework used in this research studies and also stated the the different hypothesis in this research work.
CHAPTER THREE

RESEARCH METHODOLOGY

3.0 INTRODUCTION

This chapter provides an overview of the research methodology used in this study. The methodology is used to examine and understand the predictors of student adherence to safe information security in American university of Nigeria. This chapter also covers a description of the research design, research approach, population sample, the instrumentation as well as the method of data collection.

3.1 RESEARCH DESIGN

For proper problem identification and resolution, proper research must be done. Kothari, (2004) defined research as the process by which information’s are found, gathered, examined and analyzed in order to answer a specified question that is related to a specific topic, area or field. Various advancement and knowledge acquisition by several scholars and practitioners have been achieved through several research forms (Kothari, 2004).

The research design employed in this study is the descriptive research design which entails the use of specific sample to study a phenomenon with the aim of generalizing the outcome of the sample to the entire population area. Descriptive research design is relevant here because it is all about describing people who take part in a study and depicting the participants in an accurate way. More simply put, descriptive research employs observational method; it is a method of viewing and recording the participant’s case study (Mark & Caputi Peter, 2001). The case study is an in-depth
3.2 POPULATION OF THE STUDY

The students of American University of Nigeria Yola constitute of Graduate Student and the Undergraduate Student. This population are the target population for the research study. The population cuts across the different cadres of student’s irrespective age, sex, departments or faculties or programmes. The present student population size of American University of Nigeria is 1041; this population size was gotten from the registrar’s office of American University of Nigeria. The undergraduate student constitutes 92.5% of the entire population, while the graduate students make up 7.5% of the entire population of the institution.

3.3 POPULATION AND SAMPLING

From the population size of the students of the university, a simple sampling formular was used. The following sample size equation was used.

Sample Size Equation

\[
\frac{z^2 \times p(1-p)}{e^2} \frac{1}{1+(\frac{z^2 \times p(1-p)}{e^2 N})}
\]

Equation 1 - Sample size Formula

Where \( N \) = Population Size, \( e \) = Margin Error, \( z \) = z-score.
The z-score is the standard deviation value which is a given proportion of the mean. The table below provides the z-score value.

<table>
<thead>
<tr>
<th>Confidence Level</th>
<th>z-score</th>
</tr>
</thead>
<tbody>
<tr>
<td>80%</td>
<td>1.28</td>
</tr>
<tr>
<td>85%</td>
<td>1.44</td>
</tr>
<tr>
<td>90%</td>
<td>1.65</td>
</tr>
<tr>
<td>95%</td>
<td>1.96</td>
</tr>
<tr>
<td>99%</td>
<td>2.58</td>
</tr>
</tbody>
</table>

Table 1 – Illustration of the z-score value

In other to calculate and derive the required sample size, the following parameter value were utilized.

Population size = 1041 | Margin Error = 5% | Z = 1.96.

After computing the stated figures, a sample size of 281 was derived. This figures would be used for hypothesis validation, answering the research question and also to the general objective of the study.

3.4 METHOD OF DATA COLLECTION

Data for this study was collected through primary and secondary sources of data collection. A primary data is a data that is directly collected from respondents (Kothari, 2004). Primary sources include the use of structured questionnaire to obtain information from respondents, in this case the students. Secondary sources include the collection of information from journals, newspapers, texts, and magazines relevant to behaviors concerning information security (Kothari, 2004).
3.5 RESEARCH INSTRUMENT

The research instrument for this study is a structured questionnaire which was put together to elicit information from the respondents on information security adherence behaviors. The questionnaire was created and administered to the respondents; questionnaire was designed in such a way that it contains the Likert-Scale question. The questionnaire was in two parts. Section A sought to elicit information on the demographic characteristics of the respondents while Section B contains question items needed to elicit information from the respondents on their information security adherence behaviors.

3.6 RESEARCH INSTRUMENT VALIDITY AND RELIABILITY

The research instrument was considered valid after a sample was printed out and reviewed by the project supervisor of the researcher who scrutinized the content of the instrument alongside. After much deliberation, and evaluation of the content, the instrument was considered valid for the variables it was meant to measure.

To ensure the reliability of the instrument, a test-retest reliability test was done by administering the instrument to a set of respondents and obtaining their responses. The outcome of this exercise was subjected to analysis to remove any ambiguity in the research items and therefore establish the reliability of the instrument in gathering the needed data.
3.7 ADMINISTRATION OF RESEARCH INSTRUMENT

The Questionnaire was administered to students after they were read their informed consent. A total of 276 replies was gotten before the analysis of the response; this sums up to the majority of the calculated sample size as derived.

3.8 ETHICAL CONSIDERATIONS

Permission was sought from the management of the institution for the researcher to use the respondents who were students of the institution. To avoid any ethical violation, a full declaration of the purpose of the study and the level of confidentiality required from the researcher were made known to the authority of the institutions. Respondents were also assured of absolute confidentiality in the use of information given by them.

3.9 METHOD OF DATA ANALYSIS

The Data analysis was conducted using Structural Equation Modelling (SEM) software such as SPSS 20 and also AMOS 23.0. An Exploratory factor analysis and Confirmatory factor analysis was conducted on the sample data.

The Exploratory Factor Analysis is the simplification of interrelated measures, it is used in the analysis of sample data to examine and explore the factor structure of a set of observed variables (Themessl-huber, 2014). Statistical Package for the Social Sciences (SPSS) 20.0 was used to perform the exploratory factor analysis test of the gathered data. The factor analysis, convergent validity and reliability where conducted in other to determine the adequacy of the gather sample data. For proper analysis, the Kaiser and Bartlet test, the pattern matrix, the total variance explained.
where conducted. Furthermore, for proper extraction of the factor; the maximum likelihood extraction with Promax rotation was utilized.

The Confirmatory Factor Analysis (CFA) is used for the verification of the factor structure of the observed variable. It is a statistical technique which allow researchers to test hypothesis. It illustrates the relationship that exist between observed variables and the underlying latent variables (Themessl-huber, 2014). In order to conduct the confirmatory factor analysis in this study, the Analysis of Moment Structures (AMOS) 23.0 tool was utilized. In order to properly carry out a CFA and check for the convergent and discriminant validity, tests like the model fit, significance level of the variable, composite reliability, Average variance extracted and correlation where done.
CHAPTER FOUR
DATA ANALYSIS AND FINDING

4.0 INTRODUCTION

In this chapter, the analysis of the generated data from the questionnaires which was distributed to the target population was conducted. The analysis was done for the sole purpose of achieving this research study objectives, answering the research question and for hypothesis validation. The hypothesis will also be tested based on the research model to confirm the predictor to student adherence to safe information systems security behavior in the institution of higher institution.

4.1 DEMOGRAPHIC CHARACTERISTICS OF RESPONDENTS

The undergraduate respondents constitutes 92.5% of the entire population of the American University of Nigeria, this makes the bulk sum of the respondent of the survey while the graduate student constitutes the remaining 7.5% of the entire student population of the institution. Questionnaire where administered to the target population taking into consideration missing data, invalid responses and poorly answered questionnaire. After getting the responses from the respondents, we got a total sum of 276 reliable responses; where 83% of the respondents were from the undergraduate student while 17% were from the graduate student.
<table>
<thead>
<tr>
<th>Sex</th>
<th>Frequency</th>
<th>Percentage %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>140</td>
<td>50.7</td>
</tr>
<tr>
<td>Female</td>
<td>137</td>
<td>49.6</td>
</tr>
<tr>
<td>Total</td>
<td>276</td>
<td>100</td>
</tr>
</tbody>
</table>

Table 2 - Respondents’ Distribution according to Gender

This table shows that 50.7% of the respondents were male while 49.6% of the respondents were female. This shows that majority of the respondents were male.

<table>
<thead>
<tr>
<th>Programme</th>
<th>Percentage %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Undergraduate</td>
<td>83</td>
</tr>
<tr>
<td>Graduate Student</td>
<td>17</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
</tr>
</tbody>
</table>

Table 3 - Respondents’ distribution according to programme

This table above shows that 83% of the respondents are enrolled in an undergraduate degree programmes while 17% are enrolled in a graduate degree programmes. This shows that majority of the respondents were undergraduate.

4.2 DATA ANALYSIS

The data analysis was conducted using both exploratory factor Analysis (EFA) and Confirmatory Factor Analysis (CFA) in Structural Equation Modelling (SEM) for the hypothesis testing and validation. Hair et al, (2010) suggested that structural equational Modelling (SEM) data analysis involves two major steps; the suggested steps by (Hair et al., 2010) for structural equational Modelling includes the Measurement model assessment and the structural model assessment. The Initial step of the examination of the measurement model involves the determination of convergent
and discriminate validity while the next step is to evaluate the structural model in order to establish the strength, intensity, and direction of the relationship amongst the construct in order to have a good measurement indicator (Hair et al., 2010).

4.3 COMMON METHOD VARIANCE ANALYSIS

In order to test for the common method variance analysis; the Harman's single factor test was utilized. The Harman’s single factor test is used to check if the majority of the variance in the dataset can be explained by a single factor. The % variance of any single factor should not be 50% (Podsakoff et al., 2003). The Percentage (%) variance of derived from the test is 25.459, this illustrates the validity of the dataset. This test can be used for both Exploratory Factor Analysis and Confirmatory Factor Analysis. Appendix 3 illustrates the details of the Harman common test bias.

4.4 EXPLORATORY FACTOR ANALYSIS TESTING

Maximum likelihood was carried out using Promax rotation test to examine the factors and checked if the factors would safely load together. The reliability, viability and the correlation of the factors were adequately satisfied. This analysis was adequately done for the six factors. In order to test for the sampling adequacy, the KMO and Bartlett’s test was conducted. The sampling adequacy of the data was significant as the variables loaded an acceptable value of well above 0.5; this indicates that the selected variables adequately correlates in the conducted factor analysis test. Appendix 2 provides details of the KMO and Bartlett’s test.
4.4.1 RELIABILITY AND VALIDITY

The convergent validity of the variable was determined during the analysis test generating values was well above the 0.35 threshold. The Total variance explained result showed 55.13% which is above the threshold of 50% (Hair, Black & Babin, 2010). Acceptable discriminant validity of the variables was achieved as the correlation matrix displayed correlation value of less than 0.7 thereby ensuring Safe cross loading of the factors. The details of the exploratory factor analysis, reliability and validity test are shown in Appendix 3 and 4.

4.5 CONFIRMATORY FACTOR ANALYSIS

4.5.1 THE RELIABILITY AND CONSTRUCT VALIDITY MEASUREMENT

In order to test the reliability and the construct validity following two equations were used to measure the construct reliability and extracted average variance (AVE) correspondingly.

\[
CR = \frac{\left( \sum \text{factor loading} \right)^2}{\left( \sum \text{factor loading} \right)^2 + \sum \text{measurement error}}
\]

\[
AVE = \frac{\sum \text{(factor loading)}^2}{n}
\]

Equation 2 - Composite Reliability

Equation 3 - Average Variance Extracted
In order to examine the convergent validity, we measured the average variance, the factor loading, and construct reliability discriminant validity. This can be found in the table below:

The AVE (Average Variance Extracted) was measured in order to determine the convergent validity. From the result of the factor loadings, the construct reliability and average variance extracted are illustrated in the table 6 below. Fornell & Larker (1981) stated that the recommended threshold for construct reliability and Average variance extracted is CR > 0.6 & AVE > 0.5. Fornell & Larker (1981) further stated the construct convergent validity is still adequate if that average variance extracted is less than 0.5 if the composite reliability of the construct is 0.6 and above (Fornell & Larker, 1981). In order to determine the discriminant validity, the MSV (Maximum Shared Squared Variance) must be less than Average variance extracted (AVE) (MSV<AVE) (Fornell & Larker, 1981).

The convergent validity was achieved as the AVE (Average Variance Extracted) and the CR (Composite Reliability) value where above the stated threshold of 0.5 and 0.7 respectively. Furthermore, sufficient discriminant validity was also achieved as Maximum Shared Squared Variance (MSV) was less than Average variance extracted (AVE). The table below details of the convergent and the discriminant validity.
Table 4 - Composite Reliabilities (CR), average variance extracted (AVE) and maximum shared variance (MSV)

<table>
<thead>
<tr>
<th></th>
<th>CR</th>
<th>AVE</th>
<th>MSV</th>
<th>AB</th>
<th>IN</th>
<th>TA</th>
<th>PE</th>
<th>EE</th>
<th>FC</th>
</tr>
</thead>
<tbody>
<tr>
<td>AB</td>
<td>0.765</td>
<td>0.533</td>
<td>0.089</td>
<td>0.672</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IN</td>
<td>0.744</td>
<td>0.521</td>
<td>0.028</td>
<td>0.073</td>
<td>0.703</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TA</td>
<td>0.876</td>
<td>0.644</td>
<td>0.172</td>
<td>0.226</td>
<td>0.048</td>
<td>0.803</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PE</td>
<td>0.854</td>
<td>0.595</td>
<td>0.172</td>
<td>0.299</td>
<td>0.063</td>
<td>0.415</td>
<td>0.771</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EE</td>
<td>0.818</td>
<td>0.600</td>
<td>0.028</td>
<td>0.156</td>
<td>-0.167</td>
<td>0.056</td>
<td>0.102</td>
<td>0.774</td>
<td></td>
</tr>
<tr>
<td>FC</td>
<td>0.922</td>
<td>0.798</td>
<td>0.132</td>
<td>-0.016</td>
<td>0.167</td>
<td>0.363</td>
<td>0.224</td>
<td>-0.003</td>
<td>0.893</td>
</tr>
</tbody>
</table>

4.5.2 MODEL FIT

An adequate amount of model fit was achieved. The threshold of the model indices where at the acceptable range. Table illustrate the model fit indices derived from the CFA analysis

<table>
<thead>
<tr>
<th>Fit Indices</th>
<th>Recommended value</th>
<th>Actual Value</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>χ2/df</td>
<td>&lt;3 good</td>
<td>2.287</td>
<td>(Bagozzi &amp; Yi, 1988)</td>
</tr>
<tr>
<td>AGFI</td>
<td>&gt;0.8</td>
<td>0.850</td>
<td>(Chau &amp; Hu, 2001)</td>
</tr>
<tr>
<td>RMSEA</td>
<td>&lt;0.08</td>
<td>0.065</td>
<td>(Browne &amp; Cudeck, 1993)</td>
</tr>
<tr>
<td>SRMR</td>
<td>&lt;0.9</td>
<td>0.702</td>
<td>(Hu &amp; Bentler 1999)</td>
</tr>
<tr>
<td>NFI</td>
<td>&gt;0.9</td>
<td>0.899</td>
<td>(Hair et al., 2010)</td>
</tr>
<tr>
<td>CFI</td>
<td>&gt;0.9</td>
<td>0.922</td>
<td>(Bagozzi &amp; Yi, 1988)</td>
</tr>
</tbody>
</table>

Table 5- Model fit result
4.6 HYPOTHESIS TESTING

The research model met the adequate threshold range and tolerant level. Thereafter, the relationship of the model constructs where examined in order to adequately validate the stated hypothesis. The path diagram of the model can be seen in figure 4. The path diagram illustrates the path value and the significant effect on the model.

The hypothesis test was carried out on the various variable in the model. The result showed that Threat appraisal, Performance expectance, Effort expectance have significant effect on the intention of student to adhere to safe information security behaviour; where the P value was less than the 0.05 (p<0.05). Furthermore, the result also showed that Facilitating condition also have a significant effect on the actual adherence to safe information security behavior by student; where the P value was less than the 0.05 (0.05). Intention to adhere to safe information security behavior also had a significant P value of less than 0.05; the intention to adhere to safe information security behavior significantly affect the actual adherence to safe information security behavior.
Furthermore, about 53% of variance of intention was explained by Threat appraisal, Performance expectancy, and Effort expectancy; where $R^2=0.53$. About 40% of variance of actual information security behavior was explained by the intention to adhere to safe information security behavior; where $R^2=0.40$. The table below shows the significance level of the hypothesis.

<table>
<thead>
<tr>
<th>Label</th>
<th>Estimate</th>
<th>S.E.</th>
<th>C.R.</th>
<th>P</th>
</tr>
</thead>
<tbody>
<tr>
<td>IN $\leftarrow$ TA</td>
<td>.152</td>
<td>.074</td>
<td>2.038</td>
<td>.042</td>
</tr>
<tr>
<td>IN $\leftarrow$ PE</td>
<td>.306</td>
<td>.075</td>
<td>4.080</td>
<td>***</td>
</tr>
<tr>
<td>IN $\leftarrow$ EE</td>
<td>.277</td>
<td>.051</td>
<td>5.414</td>
<td>***</td>
</tr>
<tr>
<td>AB $\leftarrow$ FC</td>
<td>-.171</td>
<td>.046</td>
<td>-3.687</td>
<td>***</td>
</tr>
<tr>
<td>AB $\leftarrow$ IN</td>
<td>1.150</td>
<td>.196</td>
<td>5.863</td>
<td>***</td>
</tr>
</tbody>
</table>

Table 6 - Shows above the significance level of the model
CHAPTER FIVE
DISCUSSION AND CONCLUSION

5.0 DISCUSSION

This study main goal is to examine the predictor of student’s adherence to safe information security behaviour in American university of Nigeria. The study utilized a research model in other to achieve it main goals and answer the research questions. The research model of the study integrates variable from the Protection Motivation theory (PMT) and Unified theory of acceptance and use of technology (UTAUT) in other to examine and investigate the phenomenon. The Protection motivation theory provides a framework for understanding the fear appeal and to understand if individuals are motivated to protect themselves against any threat and attack. The Unified Theory of Acceptance and Use of Technology (UTAUT) provides a framework that explains the behavioral intention of individuals in specific situation.

The result from the research study showed that Threat appraisal, Performance Expectancy, Effort Expectance affect the intention to adhere to safe information security behavior which invariably leads to the actual information security behavior. Furthermore, the result also showed that facilitating condition affects the actual information security behavior; thus validating the proposed hypothesis of the study. The result showed that students are willing to perform Safe information security behavior if they are well aware of their vulnerability and there is proper and safe technology or mechanism available to help prevent the compromise of the confidential and personal data. The gathered result showed that student would perform safe information security behavior if there is adequate support for them if attacked or exposed to vulnerability.
Also the study result showed that threat appraisal, performance expectancy, effort expectancy and facilitating condition are predictors of student’s adherence to safe information security behavior.

5.1 THREAT APPRAISAL

Threat appraisal is the degree to which an individual believes he/she is in danger or threatened by an event. The threat appraisal consist of the perceived vulnerability and the perceived severity. Perceived vulnerability is defined as the probability that a negative or undesirable event would occur if no preventive measure is put in place (Boer & Seydel, 1996; Rippetoe & Rogers, 1987) while perceived severity refers to the degree to which both physical and psychological damage which could occur based on the threat and or an attack (Boer & Seydel, 1996; Rippetoe & Rogers, 1987). In this study, it was proposed that threat appraisal affects students’ intention to adhere to Safe information security behavior. Threat appraisal contribute to the performance of safe information security behavior. The result of the study showed that students would willingly perform Safe information security behavior if they are aware of their exposure and vulnerability to threat and attack.

5.1.1 PERFORMANCE EXPECTANCY

Performance expectancy illustrates the users' belief of the effectiveness of using the technology (Venkatesh et al., 2003). In the context of this study, Performance expectancy refers to the student believes that adherence to safe information security behavior would help them reduce their vulnerability to threats and attack. Based on the finding derived from this study, performance expectancy influences the student intention to adhere to safe information systems security behavior. The result of this study implies that if the student does not perceive the relevance of the information security behavior to be useful, sufficient and up to date they wouldn’t perform that
information security behavior. In this study, it was proposed that Performance Expectancy affects students’ intention to adhere to safe information security behavior. Performance Expectancy contribute to the performance of safe information security behavior. The result of the study showed that student would willingly perform safe information security behavior if it would help prevent them from exposure and vulnerability to threat and attack.

5.1.2 EFFORT EXPECTANCY

It was defined has the degree of ease associated with the use of the system (Venkatesh et al., 2003). In this study, it was proposed that Effort Expectancy affects students’ intention to adhere to safe information security behavior. Effort Expectancy contribute to the performance of safe information security behavior. From the conducted literature review done in this study, it was suggested that Effort Expectancy explains the belief that an individual has the ability to protect themselves with less effort (Venkatesh et al., 2003). This research study result showed that students are willing to perform appropriate information system security behavior as long as it is easy for them to understand and use due to the motivation to protect themselves from an attack/threat.

5.1.3 FACILITATING CONDITION

Venkatesh, (2003) defined facilitating condition as the degree to which a person believes that help exist to support and make the task easy. In other words the more a resource and opportunity a person believes exist the easier it is for them to carry out a given task. In this study, it was proposed that facilitating condition affects student actual adherence to safe information security behavior. Facilitating condition contributes to the student’s actual information security behavior. The result of the study implies that if the students believes that they have adequate support that would help them would adhere to safe protective information security behavior.
5.2 IMPLICATION

In this section, we would provide both the theoretical and the practical implication of this study. The study integrates variables from the PMT (Protection Motivation Theory) UTAUT (Unified theory of acceptance and use of technology) thereby contributing to the existing field theoretically and academically. In this study, selected variables from the PMT (Protection Motivation Theory), UTAUT (Unified theory of acceptance and use of technology) were used to answer the research question and to validate the stated hypothesis; the reason for this is to have a proper understanding of the phenomenon being studied.

Protection motivation theory provides a framework for understanding the fear appeal and also to understand if individuals are motivated to protect themselves against any threat and attack. The Unified Theory of Acceptance and Use of Technology (UTAUT) provides a framework which explains the behavioral intention of individuals.

The Protection Motivation Theory (PMT) mainly focus on the fear appeal to see if individuals are motivated to protect themselves from attacks and threat. The UTAUT (Unified theory of acceptance and use of technology) as seen from the literature review conducted focuses mainly on the intention and behavior to accept and use a certain mechanism or technology. In the study, various reliability and validity test were conducted in this study for ascertaining the correctness, validity, and reliability of the model. Based on the test, the model showed an adequate level of correctness, validity, and reliability during the analysis.

The practical implication of this study is that institution of higher education in Nigeria could benefit from the result of this study. First, understanding the various predictors of student adherence to safe information security behavior would help the institution develop and implement
a useful and acceptable information systems security policies and procedure which would be effective and efficient to the institution and all the stakeholders.

Finally, it would help the institution to design good educational and awareness mechanisms for the students in other to provide them with awareness and education about different vulnerabilities, threat and attack them and the institution is faced with.

5.3 LIMITATION

This study isn’t without limitation; there are various limitations with regards to this research study. First, variable such as Social Influence (SI) in the UTAUT theory was not used. During the study, it became evident that this variable could be used; Social Influence (SI) illustrates how individual decision making is affected by significant other perception. This variable could be added to the research model for a more extensive view of the Predictors of student to adhere to safe information security behavior.

Second, the study did not consider the different age categories. Further research could compare the age categories

5.4 SUGGESTION FOR STUDY

This study is one of the few research studies that integrates variables from the Protection Motivation Theory (PMT) and Unified theory of acceptance and use of technology theory (UTAUT) in the context of the information security. However, there are several suggestions for further research.

First, the Future study should include variable such as Social Influence (SI) from the UTAUT (Unified theory of acceptance and use of technology) theory in other to understand the influence a
significant other has on an individual when an individual is making adherence decision about information security behavior.

Secondly, Future research study should include the different age categories of the respondent in other to ascertain the maturity level of the respondent.

Finally, future research should conduct this research using a population of higher density and a different higher educational setting.

5.5 CONCLUSION

In institution of higher education, it is important to understand the student behavior to information security for adequately and effective development of information security procedures, mechanisms and policies. This study examined the student adherence to safe information security behavior and predictors that affect student adherence to safe information security behavioral practise.

In this study, specific variables from the Protection Motivation Theory (PMT) and the UTAUT (Unified theory of acceptance and use of technology) were utilized for the hypothesis validation and to also answer the research.

In other to achieve an effective information security, there is need to adequately understand the human and technological facet of information security. For insurance of safe and effective individual behavior, information security measure would help ensure successful protection of data and information from data and information compromise.

Proper understanding of the predictors to safe information security would help promote information security awareness and education; this would help ensure adequate and effective information security.
REFERENCE


https://doi.org/10.2307/1252146


https://doi.org/10.1016/S0167-4048(01)00507-7


ViswanathVenkatesh, Michael G. Morris, Gordon B. Davis, F. D. D., Venkatesh, V., Morris,


Yusuf, M., Oluwole, A., & Loto, A. (2013). Appraising the role of information communication

https://doi.org/10.5897/IJEAPS12.027

APPENDICES

APPENDIX 1: SURVEY QUESTION

SURVEY ON STUDENT’S PERCEPTION OF INFORMATION SYSTEM SECURITY AT AMERICAN UNIVERSITY OF NIGERIA, YOLA

Please Click the appropriate number to indicate the level of your agreement or disagreement with your perception of Information system security on a scale of 1 to 5, where 1 = Completely Disagree, 2 = Disagree, 3 = Neutral (neither disagree nor agree), 4 = Agree, and 5 = Completely agree.

Questionnaire

Informed Consent

Title of Research: Information security Adherence in institutions of higher education: A student Perspective

Principal Researcher Name: ODEGBESAN OMOBO LAJI AYOMIDE

Title: Master Institution: American university of Nigeria (AUN)

Location: 98 Lamido Zubairu Way Yola Township bypass PMB 2250, Yola Adamawa State, Nigeria

Research Supervisor Name: Salihu Ibrahim Dasuki (PhD)

Institution: American university of Nigeria (AUN)

Location: 98 Lamido Zubairu Way Yola Township bypass PMB 2250, Yola Adamawa State, Nigeria

Invitation

You are invited to participate in a masters research study in information systems at the American University of Nigeria, this as a result of you been the target population of the research. Your response would provide the necessary data which would then be analyzed for hypothesis confirmation and also provision of empirical evidence for the study.

Research Purpose The goal of this research is to investigate and examine the various factors that influences the student intention to adhere with information security in an institution of higher education.

Description of Procedures Your involvement in this research will take place through an online survey instrument such as google form that will last approximately 2weeks

Confidentiality and Anonymity Your identity will remain anonymous throughout the research process and will not be disclosed at any time. All interview materials will be safely
stored. The data would also be stored in an offline device which would be protected by password. The files would be adequately encrypted and backed up on the ICLOUD in other to prevent loss and for proper protection. The information you share in the interview would be used for the researcher’s Masters degree in information systems at the American University of Nigeria, as well as subsequent publications in journals, books, and presentations. Your name and identity will remain anonymous in all materials.

Potential Risks

There are no potential or foreseeable risks involved with this study.

Potential Benefits to Participants or to Society It is anticipated that the outcomes of the study will help institutions especially that of higher education to understand major reason for students intentions toward to information security and the necessary action that would be used to tackle the problem

Participation is Voluntary Your participation in this study is completely voluntary. You are free to decide if you wish to participate. You may withdraw from the study at any point and for any reason.

During the research, if there is a question that you do not wish to answer, you may decline to do so and remain in the study. At any point in the research process, including during your interview, you may ask questions for clarification or seek new information.

Who to contact with questions:

Principal Investigator:
Name: ODEGBESAN OMOBOLAJI AYOMIDE
Institution: American university of Nigeria (AUN)
Location: 98 Lamido Zubairu Way Yola Township bypass PMB 2250, Yola Adamawa State, Nigeria
Telephone contact: +2347060649404
E-mail: Bolaji.odegbesan@aun.edu.ng

Research Supervisor: Name: Salihu Ibrahim Dasuki (PhD)
Institution: American university of Nigeria (AUN)
Location: 98 Lamido Zubairu Way Yola Township bypass PMB 2250, Yola Adamawa State, Nigeria
Telephone contact: +2349052522657
E-mail: salihu.dasuki@aun.edu.ng

If you feel like speaking to someone else about the research and the findings, you may contact the AUN Institutional Review Board at irb@aun.edu.ng.
Demographic

Gender *
- [ ] Female
- [x] Male

Educational Level *
- [ ] Undergraduate
- [x] Masters
- [ ] PHD

Threat Appraisal

My personal information might be exposed to threat and attack due to lack of adequate security technology *

1 2 3 4 5
Strongly Disagree □ □ □ □ □ | Strongly Agree

My personal information is likely to be compromise by virus and malware *

1 2 3 4 5
Strongly Disagree □ □ □ □ □ | Strongly Agree

The loss of my personal information would be a serious problem for me *

1 2 3 4 5
Strongly Disagree □ □ □ □ □ | Strongly Agree

Critical and personal data compromise would be a serious problem for me *

1 2 3 4 5
Strongly Disagree □ □ □ □ □ | Strongly Agree

Performance Expectancy

The use of information security technology effectively protect my critical and personal information *
Ensuring proper safe guard is the protection of my personal information *

Ensuring proper information security measure on my system effectively prevent my system from violation*

Proper use of information security measure prevent me from data compromise *

Effort Expectancy

It is easy to use information security technology tools *

I can easily ensure proper information security protection against virus *

I can perform proper information security preventive measure easily *

I can easily access information security technology *
Facilitating Condition

I have the necessary and required information about the information system security measures *

1 2 3 4 5

| Strongly Disagree | | | | | Strongly Agree |

There is a specific person (or group) who is available to assist me with difficult information security Procedures *

1 2 3 4 5

| Strongly Disagree | | | | | Strongly Agree |

I have the necessary Knowledge to carry out the information security measures *

1 2 3 4 5

| Strongly Disagree | | | | | Strongly Agree |

Necessary materials are available to help me understand and implement the information security measure *

1 2 3 4 5

| Strongly Disagree | | | | | Strongly Agree |

Intention

I will ensure preventive measure against information security violation *

1 2 3 4 5

| Strongly Disagree | | | | | Strongly Agree |

I will utilize information security technology *

1 2 3 4 5

| Strongly Disagree | | | | | Strongly Agree |
I will never make use of unreliable Software on my system *

1 2 3 4 5

Strongly Disagree [ ] [ ] [ ] [ ] [ ] Strongly Agree

I will perform proper information security measure *

1 2 3 4 5

Strongly Disagree [ ] [ ] [ ] [ ] [ ] Strongly Agree

**Actual Behavior**

I use Information security Technology to protect my personal and confidential information *

1 2 3 4 5

Strongly Disagree [ ] [ ] [ ] [ ] [ ] Strongly Agree

I never share and disclose my login credentials with anyone *

1 2 3 4 5

Strongly Disagree [ ] [ ] [ ] [ ] [ ] Strongly Agree

I promptly delete suspicious email without opening them *

1 2 3 4 5

Strongly Disagree [ ] [ ] [ ] [ ] [ ] Strongly Agree

I regularly scan and remove virus and malicious software from my system *

1 2 3 4 5

Strongly Disagree [ ] [ ] [ ] [ ] [ ] Strongly Agree
## APPENDIX 2: PATTERN MATRIX

**Pattern Matrix**

<table>
<thead>
<tr>
<th></th>
<th>Factor 1</th>
<th>Factor 2</th>
<th>Factor 3</th>
<th>Factor 4</th>
<th>Factor 5</th>
<th>Factor 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>EE4</td>
<td>.910</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EE1</td>
<td>.855</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EE3</td>
<td>.742</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EE2</td>
<td>.644</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PE2</td>
<td></td>
<td>.966</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PE3</td>
<td></td>
<td>.878</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PE1</td>
<td></td>
<td>.788</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PE4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC1</td>
<td></td>
<td></td>
<td>.765</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC3</td>
<td></td>
<td></td>
<td>.731</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC2</td>
<td></td>
<td></td>
<td>.612</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC4</td>
<td></td>
<td></td>
<td>.610</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC2</td>
<td></td>
<td></td>
<td></td>
<td>.968</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC1</td>
<td></td>
<td></td>
<td></td>
<td>.886</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC3</td>
<td></td>
<td></td>
<td></td>
<td>.831</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IN3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>.541</td>
<td></td>
</tr>
<tr>
<td>IN1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>.513</td>
<td></td>
</tr>
<tr>
<td>IN2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>.635</td>
<td></td>
</tr>
<tr>
<td>T3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>.817</td>
</tr>
<tr>
<td>T2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>.705</td>
</tr>
<tr>
<td>T4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>.649</td>
</tr>
<tr>
<td>T1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Extraction Method: Maximum Likelihood.

Rotation Method: Promax with Kaiser Normalization.

a. Rotation converged in 6 iterations.
## APPENDIX 3: COMMON METHOD VARIANCE TEST

<table>
<thead>
<tr>
<th>Component</th>
<th>Initial Eigenvalues</th>
<th>Extraction Sums of Squared Loadings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Total</td>
<td>% of Variance</td>
</tr>
<tr>
<td>2</td>
<td>2.900</td>
<td>13.180</td>
</tr>
<tr>
<td>3</td>
<td>2.134</td>
<td>9.698</td>
</tr>
<tr>
<td>4</td>
<td>1.768</td>
<td>8.036</td>
</tr>
<tr>
<td>5</td>
<td>1.693</td>
<td>7.695</td>
</tr>
<tr>
<td>6</td>
<td>.895</td>
<td>4.069</td>
</tr>
<tr>
<td>7</td>
<td>.869</td>
<td>3.951</td>
</tr>
<tr>
<td>8</td>
<td>.714</td>
<td>3.246</td>
</tr>
<tr>
<td>9</td>
<td>.631</td>
<td>2.866</td>
</tr>
<tr>
<td>10</td>
<td>.604</td>
<td>2.745</td>
</tr>
<tr>
<td>11</td>
<td>.549</td>
<td>2.495</td>
</tr>
<tr>
<td>12</td>
<td>.501</td>
<td>2.277</td>
</tr>
<tr>
<td>13</td>
<td>.456</td>
<td>2.075</td>
</tr>
<tr>
<td>14</td>
<td>.433</td>
<td>1.967</td>
</tr>
<tr>
<td>15</td>
<td>.418</td>
<td>1.899</td>
</tr>
<tr>
<td>16</td>
<td>.385</td>
<td>1.750</td>
</tr>
<tr>
<td>17</td>
<td>.334</td>
<td>1.520</td>
</tr>
<tr>
<td>18</td>
<td>.315</td>
<td>1.432</td>
</tr>
<tr>
<td>19</td>
<td>.265</td>
<td>1.206</td>
</tr>
<tr>
<td>20</td>
<td>.224</td>
<td>1.020</td>
</tr>
<tr>
<td>21</td>
<td>.170</td>
<td>.774</td>
</tr>
<tr>
<td>22</td>
<td>.141</td>
<td>.642</td>
</tr>
</tbody>
</table>

Extraction Method: Principal Component Analysis.
APPENDIX 4: KMO AND BARTLETT'S TEST AND TOTAL VARIANCE EXPLAINED

KMO and Bartlett's Test

<table>
<thead>
<tr>
<th></th>
<th>Kaiser-Meyer-Olkin Measure of Sampling Adequacy</th>
<th>Approx. Chi-Square</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>.831</td>
<td>2788.924</td>
</tr>
<tr>
<td>Bartlett's Test of Sphericity</td>
<td>df</td>
<td>231</td>
</tr>
<tr>
<td></td>
<td>Sig.</td>
<td>.000</td>
</tr>
</tbody>
</table>

Total Variance Explained

<table>
<thead>
<tr>
<th>Factor</th>
<th>Initial Eigenvalues</th>
<th>Extraction Sums of Squared Loadings</th>
<th>Rotation Sums of Squared Loadingsa</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Total</td>
<td>% of Variance</td>
<td>Cumulative %</td>
</tr>
<tr>
<td>1</td>
<td>5.601</td>
<td>25.459</td>
<td>25.459</td>
</tr>
<tr>
<td>3</td>
<td>2.134</td>
<td>9.698</td>
<td>48.337</td>
</tr>
<tr>
<td>4</td>
<td>1.768</td>
<td>8.036</td>
<td>56.372</td>
</tr>
<tr>
<td>5</td>
<td>1.693</td>
<td>7.695</td>
<td>64.067</td>
</tr>
<tr>
<td>6</td>
<td>.895</td>
<td>4.069</td>
<td>68.136</td>
</tr>
<tr>
<td>7</td>
<td>.869</td>
<td>3.951</td>
<td>72.087</td>
</tr>
<tr>
<td>8</td>
<td>.714</td>
<td>3.246</td>
<td>75.333</td>
</tr>
<tr>
<td>9</td>
<td>.631</td>
<td>2.866</td>
<td>78.200</td>
</tr>
<tr>
<td>10</td>
<td>.604</td>
<td>2.745</td>
<td>80.944</td>
</tr>
<tr>
<td>11</td>
<td>.549</td>
<td>2.495</td>
<td>83.439</td>
</tr>
<tr>
<td>12</td>
<td>.501</td>
<td>2.277</td>
<td>85.716</td>
</tr>
<tr>
<td>13</td>
<td>.456</td>
<td>2.075</td>
<td>87.791</td>
</tr>
<tr>
<td>14</td>
<td>.433</td>
<td>1.967</td>
<td>89.758</td>
</tr>
<tr>
<td>15</td>
<td>.418</td>
<td>1.899</td>
<td>91.657</td>
</tr>
<tr>
<td>16</td>
<td>.385</td>
<td>1.750</td>
<td>93.406</td>
</tr>
<tr>
<td>17</td>
<td>.334</td>
<td>1.520</td>
<td>94.927</td>
</tr>
<tr>
<td>18</td>
<td>.315</td>
<td>1.432</td>
<td>96.359</td>
</tr>
<tr>
<td>19</td>
<td>.265</td>
<td>1.206</td>
<td>97.564</td>
</tr>
<tr>
<td>20</td>
<td>.224</td>
<td>1.020</td>
<td>98.584</td>
</tr>
<tr>
<td>21</td>
<td>.170</td>
<td>.774</td>
<td>99.358</td>
</tr>
<tr>
<td>22</td>
<td>.141</td>
<td>.642</td>
<td>100.000</td>
</tr>
</tbody>
</table>

Extraction Method: Maximum Likelihood.

a. When factors are correlated, sums of squared loadings cannot be added to obtain a total variance.