Invention Journal of Research Technology in Engineering & Management (IJRTEM)
ISSN: 2455-3689
www.ijrtem.com Volume 3 Issue 2 ǁ February 2019 ǁ PP 47-56

Information Security Adherence in Institutions of Higher Education: A Case Study of American University of Nigeria

[1,]Odegbesan Omobolaji Ayomide, [2,]Kolapo Ridwan Olayinka

[1,] Department of Information systems, American University of Nigeria, Nigeria[1],
[2,] Computer and physical sciences department, Lead City university, Ibadan[2].

ABSTRACT: Institutions 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 behavior in institutions 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 students to practice safe information security behavior. This study utilized the quantitative research method for data gathering and analysis. A total of 276 responses were gotten from the respondents. The result showed that the threat appraisal, performance expectancy, effort Expectancy have a significant impact on the intention to adhere to a safe information security behavior. While facilitating condition have a significant impact on actual protection, and also the intention has 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 influences safe information security behavior.

I. INTRODUCTION

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 [1]; due to this, information protection and security have become a critical issue. The need for the protection of information and its assets have become paramount in institutions and organization [2]. However, institutions and organization must ensure that proper information security practice becomes 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 [3]. The primary objective of information security in institutions includes the prevention, avoidance, detection, and recovery of information and its essential asset [4]. 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 [5]. Information security cut across hardware, software, threats and challenges, physical security and also human behavior. However, there is a need to understand every aspect of information security in other to proffer effective and efficient information security measure and procedure for adequate protection of information and its assets.

Furthermore, the increased accessibility to information and its asset have led to a high susceptibility level to threats, and attacks. Also, high vulnerability to the threat and attacks have made the tightening of information security a significant priority in organizations and institution [6], [7]. The security attainment and the utilization of technology are not sufficient enough to ensure adequate information security; consideration has to be given to the organization and institution itself [8]. 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 [9]. 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 other remote[11], [12]. For several decades, information security and confidentiality in institutions of higher education have been a significant concern [2], [5]. The institution of higher education has 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 institutions of higher education are not only designed to serve the needs of staffs, student and faculty alone but also to serve and accommodate the needs of guests and researchers. While the nature of higher educational institution involves openness and transparency to the public and constant distribution of information, a balance must be maintained in other to ensure that information assets are not exposed to risk or compromised [14]. A breach in a universities' information asset can undermine its integrity and growth. In the context of the higher educational institutions, there is a need to properly understand Information security threats and challenges facing higher education institutions in other to prevent potential loss of information and knowledge assets [2].

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 literature on information security in the institutions of higher education are technical with little consideration on institutional and individual issues and behavior [15]. Many institutions do not pay attention to the individual behavior and value of information security. However, a 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 need to be aware of the necessity of understanding the institutional and individual behavior and issues alongside the technical facet of information security [2]. The technical and non-technical facet of information security should be balanced while continuous improvement and learning is ensured [16].In this study, the American University of Nigeria (AUN) has been chosen as a case study. The American University of Nigeria is among several number institutions with a 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.

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 the AmericanUniversity 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 the American University of Nigeria.
- To examine the predictors that affect student adherence to safe information security practice in the American University of Nigeria.
- To examine the student's information security behavior in the American University of Nigeria

Research Question

- What are the predictors of student adherence to safe information security behavior in institutions of higher education in Nigeria using the AmericanUniversity of Nigeria?
- To what extent do student perform safe information security behavior in the American University of Nigeria?

II. METHOD

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 [17]. The research design employed in this study is the descriptive research design which entails the use of a specific sample to study a phenomenon with the aim of generalizing the outcome of the sample to the entire population area. The 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 [18]. The case study is an in-depth study of an individual or group of individuals and survey, defined as a brief interview or discussion with an individual about a specific topic. The students of the American University of Nigeria Yola constitute of Graduate Student and the Undergraduate Student. This population is 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.

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

Sample Size Equation

$$\frac{\frac{z^2 \times p(1-p)}{e^2}}{1+\left(\frac{z^2 \times p(1-p)}{e^2 N}\right)}$$

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.

Confidence Level	z-score
80%	1.28
85%	1.44
90%	1.65
95%	1.96
99%	2.58

Table 1 – Illustration of the z-score value

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

Data for this study was collected through primary and secondary sources of data collection. Primary data is data that is directly collected from respondents. Primary sources include the use of a 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 [17]. 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; the 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.

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. 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 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 was made known to the authority of the institutions. Respondents were also assured of absolute confidentiality in the use of information given by them. The Data analysis was conducted using Structural Equation Modelling (SEM) software such as SPSS 20 and also AMOS 23.0. 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 [19]. 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 were 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 allows researchers to test the hypothesis. It illustrates the relationship that exists between observed variables and the underlying latent variables [19]. In other to conduct the confirmatory factor analysis in this study, the Analysis of Moment Structures (AMOS) 23.0 tool was utilized. In other to properly carry out a CFA and check for the convergent and discriminant validity, a test like the model fit, a significance level of the variable, composite reliability, Average variance extracted and correlation where done.

III. RESULT

Introduction: In this chapter, the analysis of the generated data from the questionnaires which were distributed to the target population was conducted. The analysis was done for the sole purpose of achieving these 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. The undergraduate respondents constitute 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. Questionnaires were 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.

Sex	Frequency	Percentage %
Male	140	50.7
Female	137	49.6
Total	**276**	**100**

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.

Programme	Percentage %
Undergraduate	83
Graduate Student	17
Total	**100**

Table 3 - Respondents' distribution according to the programme

This table above shows that 83% of the respondents are enrolled in undergraduate degree programmes while 17% are enrolled in graduate degree programmes. This shows that majority of the respondents were undergraduate. 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 significant 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 other to establish the strength, intensity, and direction of the relationship amongst the construct in other to have a good measurement indicator (Hair et al., 2010).

Common Method Variance Analysis: In other to test for the common method variance analysis; 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 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.

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 other to test for the sampling adequacy, the KMO and Bartlett’s test was conducted. The sampling adequacy of the data was significant has 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.

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

$$CR= (\sum \text{factor loading})\ 2 / ((\sum \text{factor loading})\ 2 + \sum \text{measurement error})$$

Equation 2 - Composite Reliability

$$AVE=\sum (\text{factor loading})\ 2/n$$

Equation 3 - Average Variance Extracted

In other 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 other to determine the convergent validity. From the result of the factor loadings, the construct reliability and average variance extracted are illustrated in 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 that 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 [22]. In other to determine the discriminant validity, the MSV (Maximum Shared Squared Variance) must be less than the Average variance extracted (AVE) (MSV<AVE) [22].

The convergent validity was achieved as the AVE (Average Variance Extracted) and the CR (Composite Reliability) values was 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 the Average variance extracted (AVE). The table below details of the convergent and the discriminant validity.

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

Table 4 - Composite Reliabilities (CR), average variance extracted (AVE) and maximum shared variance (MSV)

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

Fit Indices	**Recommended value**	**Actual Value**	**Author**
χ2/df	<3 good	2.287	[23]
AGFI	>0.8	0.850	[24]
RMSEA	<0.08	0.065	[25]
SRMR	<0.9	0.702	(Hu &Bentler 1999)
NFI	>0.9	0.899	[20]
CFI	>0.9	0.922	[23]

Table 5- the Model fit result

Hypothesis Testing: The research model met the adequate threshold range and a tolerant level. After that, the relationship of the model constructs was examined in other 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 expectancy, Effort expectancy have a significant effect on the intention of the student to adhere to safe information security behavior; where the P value was less than the 0.05 ($p<0.05$). Furthermore, the result also showed that Facilitating condition also has a significant effect on the actual adherence to safe information security behavior by the student; where the P value was less than 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.

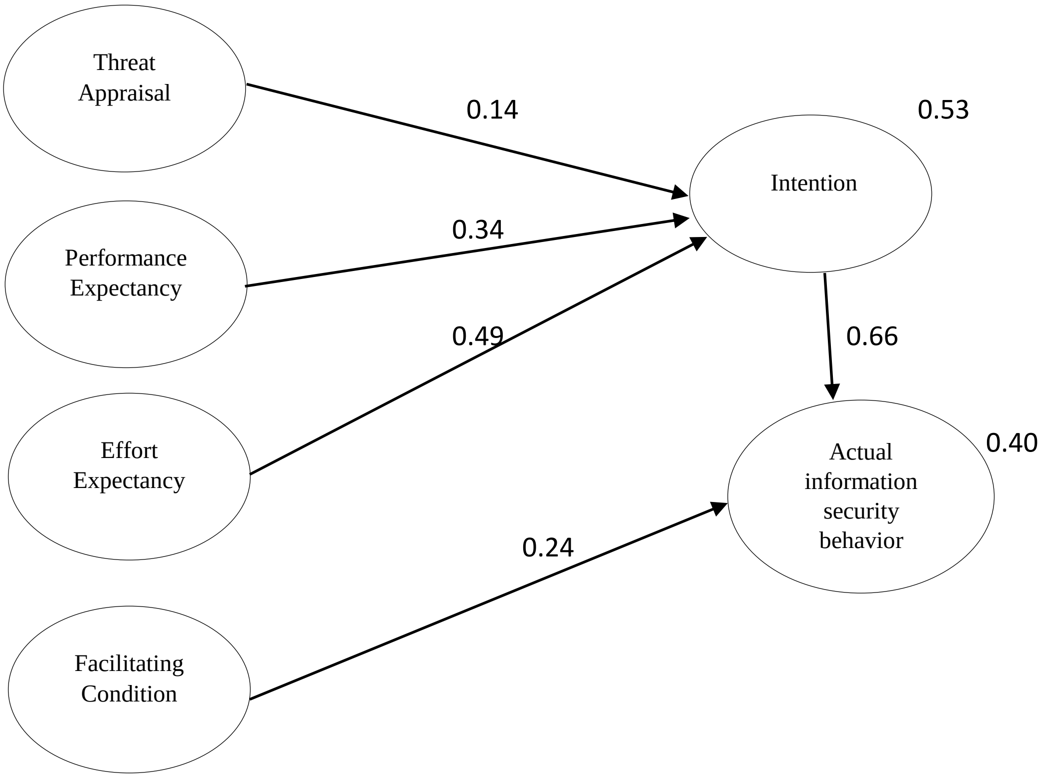

Figure 1 - Research Model Path Diagram

Furthermore, about 53% of the variance of intention was explained by Threat appraisal, Performance expectancy, and Effort expectancy; where R2=0.53. About 40% of the variance of actual information security behavior was explained by the intention to adhere to safe information security behavior; where R2=40. The table below shows the significance level of the hypothesis.

			Estimate	S.E.	C.R.	P	Label
IN	<---	TA	.152	.074	2.038	.042	
IN	<---	PE	.306	.075	4.080	***	
IN	<---	EE	.277	.051	5.414	***	
AB	<---	FC	-.171	.046	-3.687	***	
AB	<---	IN	1.150	.196	5.863	***	

Table 6 - Shows above the significance level of the model

IV. DISCUSSION AND CONCLUSION

This main study goal is to examine the predictor of student's adherence to safe information security behavior in the American University of Nigeria. The study utilized a research model in other to achieve its 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 a specific situation. The result from the research study showed that Threat appraisal, Performance Expectancy, Effort Expectancy 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.

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 consists of perceived vulnerability and perceived severity. Perceived vulnerability is defined as the probability that a harmful or undesirable event would occur if no preventive measure is put in place [26], [27] while perceived severity refers to the degree to which both physic and psychological damage which could occur based on the threat and or an attack [26], [27]. In this study, it was proposed that threat appraisal affects students' intention to adhere to Safe information security behavior. Threat appraisal contributes 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.

Performance Expectancy: Performance expectancy illustrates the users' belief of the effectiveness of using the technology [28]. 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 would not 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 contributes 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.

Effort Expectancy: It was defined as 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 contributes 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 can protect themselves with less effort [28]. 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.

Facilitating Condition: Venkatesh, (2003) defined facilitating condition as the degree to which a person believes that help exists 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 believe that they have adequate support that would help them would adhere to safe, protective information security behavior.

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 specific mechanism or technology. In the study, various reliability and validity test was 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 proper education 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.

Limitation: This study is not 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 the 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

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.

V. CONCLUSION

In institutions of higher education, it is essential to understand the student behavior to information security for adequately and active development of information security procedures, mechanisms, and policies. This study examined students adherence to safe information security behavior and predictors that affect student adherence to safe information security behavioral practice. 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 effective information security, there is a need to understand the human and technological facet of information security adequately. 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. A 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

[1] C. A. Varney, “Consumer Privacy In the Information Age: A View From the United States,” 1996. [Online]. Available: https://www.ftc.gov/es/public-statements/1996/10/consumer-privacy-information-age-view-united-states. [Accessed: 19-Mar-2017].

[2] A. A. Marks, “Exploring universities’ information systems security awareness in a changing higher education environment : a comparative case study research,” no. June 2007.

[3] M. E. Whitman and H. J. Mattord, “Introduction to Information Security,” *Princ. Inf. Secur.*, pp. 1–38, 2011.

[4] H. a H. Awad and F. M. Battah, “Enhancing Information Systems Security in Educational Organizations in KSA through proposing security model,” *Int. J. Comput. Sci. Issues*, vol. 8, no. 5, pp. 354–358, 2011.

[5] B. W. Okibo and O. B. Ochiche, “Challenges Facing Information Systems Security Management in Higher Learning Institutions : A Case Study of the Catholic University of Eastern Africa – Kenya,” vol. 3, no. 1, pp. 336–349, 2014.

[6] J. Seely and P. Duguid, “The Social Life of Information,” 2000.

[7] M. Al-awadi and K. Renaud, “Success factors in information security: implementation in organizations,” *ADIS Int. Conf. e-Society*, pp. 169–176, 2007.

[8] A. Segev, J. Porra, and M. Roldan, “Internet Security AND THE CASE OF BANK OF AMERICA.,” *Commun. ACM*, vol. 41, no. 10, pp. 81–87, 1998.

[9] C. M. Trompeter and J. H. P. Eloff, “A framework for the implementation of socio-ethical controls in information security,” *Comput. Secur.*, vol. 20, no. 5, pp. 384–391, 2001.

[10] M. N. Harrell, “Factors impacting information security noncompliance when completing job tasks,” no.

21, 2014.

[11] CERT, “2014 U.S. State of Cybercrime Survey,” 2014.

[12] Pwc, “State of Cybercrime Survey 2013,” p. 20, 2013.

[13] F. H. Katz and F. H. Katz, “The effect of a university information security survey on instruction methods in information security The Effect of a University Information Security Survey on Instruction Methods in Information Security,” no. July, 2005.

[14] B. Smith, “Information Security Incident Management,” *Inf. Secur. Fundam.*, vol. 3, no. 3, pp. 257–280, 2013.

[15] V. Mahabi, “Information security awareness: System administrators and end-user perspectives at Florida State University,” *ProQuest Diss. Theses*, p. 144, 2010.

[16] Y. Rezgui and A. Marks, “Information security awareness in higher education: An exploratory study,” *Comput. Secur.*, vol. 27, no. 7–8, pp. 241–253, 2008.

[17] C. R. Kothari, *Research Methodology: Methods & Techniques*. 2004.

[18] B. Mark and Caputi Peter, “Introduction to quantitative research,” *SAGE Publ. Ltd*, p. 272, 2001.

[19] M. Themessl-huber, “Evaluation of the ^{2}-statistic and different fit-indices under misspecified number of factors in confirmatory factor analysis,” *Psychol. Test Assess. Model.*, vol. 56, no. 3, pp. 219–236, 2014.

[20] J. F. Hair, W. C. Black, B. J. Babin, and R. E. Anderson, “Multivariate Data Analysis,” *Vectors*. p. 816, 2010.

[21] P. M. Podsakoff, S. B. MacKenzie, J.-Y. Lee, and N. P. Podsakoff, “Common method biases in behavioral research: A critical review of the literature and recommended remedies.,” *J. Appl. Psychol.*, vol. 88, no. 5, pp. 879–903, 2003.

[22] C. Fornell and D. F. Larcker, “Evaluating Structural Equation Models with Unobservable Variables and Measurement Error,” *J. Mark. Res.*, vol. 18, no. 1, p. 39, 1981.

[23] R. P. Bagozzi and Y. Yi, “On the Evaluation of Structural Equation Models,” *Journal of the Academy of Marketing Science*, vol. 16, no. 1. pp. 74–94, 1988.

[24] P. Y. K. Chau and P. J.-H. Hu, “Information Technology Acceptance by Individual Professionals: A Model Comparison Approach*,” *Decis. Sci.*, vol. 32, no. 4, pp. 699–719, 2001.

[25] M. W. Browne and R. Cudeck, “Alternative ways of assessing model fit,” *Sage Focus Ed.*, vol. 154, p. 136, 1993.

[26] P. A. Rippetoe and R. W. Rogers, “Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat.,” *Journal of Personality and Social Psychology*, vol. 52, no. 3. American Psychological Association, US, pp. 596–604, 1987.

[27] H. Boer and E. R. Seydel, “Protection motivation theory,” *Predicting Health Behavior: Research and Practice with Social Cognition Models*. pp. 95–120, 1996.

[28] V. Venkatesh, M. Hall, G. B. Davis, F. D.. Davis, S. M. Walton, and M. G.. Morris, “User Acceptance of Information Technology: Toward a Unified,” *MIS Q.*, vol. 27, no. 3, pp. 425–478, 2003.

[29] F. D. . D. Viswanath Venkatesh, Michael G . Morris, Gordon B. Davis, V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, “User acceptance of information technology: Toward a unified view,” *MIS Q.*, vol. 27, no. 3, pp. 425–478, 2003.