Vol. 12, No. 3, September 2019, pp. 61 - 73 *ISSN 2006-1781*
Adedayo Solomon Williams, Folakemi Akinbohun, Olusegun Mathew Awotunde and Olojido Joseph Bamikole (2019), An Empirical Investigation into the Relationship between Motivational Factors and Threats Consciousness among Some Malaysian Postgraduate Students

An Empirical Investigation into the Relationship between Motivational Factors and Threats Consciousness among some Malaysian Postgraduate Students

Adedayo Solomon Williams[1], Folake akinbohun[2] and Olusegun Mathew Awotunde[3] Olojido Joseph Bamikole[4]

School of Management, IT & Governance,
University of KwaZulu-Natal, Westville Campus, Durban,
South Africa
Email: [1]ladwillylibrary@gmail.com, [2]folakeakinbohun@yahoo.com, [3]awotundemo@gmail.com, 4olojidoj@gmail.com

ABSTRACT

The increasing growth of information technology tools in this digital age has made the experience of information security threats prominent. Qualities of information such as integrity, availability and confidentiality are consistently being lost, with frequent access to the data repository is endangering confidentiality. This unfortunate experience of information security threats is not limited to national security but also experienced in commerce and finance, as well as academic institutions. There has been reported a series of information breaches amongst student in university, despite policies and rules put in place protecting university information systems. The aim of this study is to the emphasis the factors promoting information security threats consciousness amongst university students. The study identified the perceived severity of the threats, information security policy compliance and information security awareness to have a relationship with information security threats consciousness. Academic communities with students, lecturers and tutors as principal users of information are specifically experiencing information security threats, but few studies have been conducted to address this development. Amongst these few studies are conceptual reviews and empirical works that did not examine the motivational factors of information security and their relationship with information security threats amongst students. To attend to this, this study employs a quantitative approach with Pearson Correlation as the statistical technique to investigate the relationship between motivational factors and information security threats amongst students. The findings of this study showed that awareness, perceived threats severity and information security policy compliance are information security motivational factors, which are positively related to information security threats.

Keyword- *information security threats; information security policies; perceived threats severity*

African Journal of Computing & ICT Reference Format:

Adedayo Solomon Williams, Folakemi Akinbohun, Olusegun Mathew Awotunde and Olojido Joseph Bamikole (2019), An Empirical Investigation into the Relationship between Motivational Factors and Threats Consciousness among Some Malaysian Postgraduate Students, *Afr. J. Comp. & ICT*, Vol.12, No. 3, pp. 61 - 73.

I. INTRODUCTION

Information has been integrated into the World Wide Web and the system of web-based integrated information systems through networks permits every organization to share their respective information and collaborate with others. As a result of this, the information of organizations is vulnerable [40]. However, the use of information security compliance refers to the achievement of information security standards and policies for protecting information in organizations [3]. Information security is the act, technology and, behavior put in place to secure individual and corporate information amongst information security threats. Furthermore, the usage of information security constantly guarantees that information security systems can cooperate successfully to ensure and protect the basic information needed by individuals and organizations [18]. The context of information security can never be ruled out in the modern age, as access to information technology increases every day.

To ensure that information and other related resources are secured, a set of information security policies has been put in place. Interestingly, information security is accomplished through various controls, including authoritative structures, strategies, systems and innovations.

Many problems and threats have been faced by individuals and organizations with regard to the security and protection of information. Such problems have militated against the achievement of objectives by individuals and organizations. In addition, it was found by [15] that most organizations are facing different obstacles in protecting their information, compounded by the increasing complexity, interconnections, uncertainties and dependence on technology. [1] stated that there is a need to protect information and knowledge which are important to the activities of individuals and organizations. [38] examined the factors related to normative beliefs, threat appraisal, self-efficacy and visibility, all of which influence employees' intention to comply with information security policies in organizations. [18] examines the social impact of changing an individual's thoughts, actions, feelings, attitudes and behaviors on information security compliance in organizations. [46] identified the different ways used by criminals in attacking individual and organizational information, including malware and vulnerabilities. This is leading to a lack of interest by the users who no longer have confidence in any anti-virus or software. Additionally, [17] stated that 95% of the attacks on information were significant to home users. This shows that individual users are the most targeted for attack, hence is a need for protection. In addition, [12] and [16] explored the security of personal computer users and organizations. The study found that the internet structure allowed for many security threats to occur. The conclusion of the study is that confidentiality, integrity, privacy and availability have direct and indirect significance on the security of the user's computer in the student community. The adoption of information security measures must be addressed by a theory that considers the influence of external factors, which is consistent with the Institutional Theory [21], a theoretical approach that is common in studies of the social sciences and suggested for studies on Information Security by different authors, such as [27] and [4].

[26] Perceived severity explains the extent to which a person perceived a serious effect on information security, which may be caused by information security breaches. From the words of the author, many types of research have been conducted, bordering on health protection motivation. This theory has laid claim to being a substantial theoretical and empirical explanation pertaining to the behaviors amongst patients. Furthermore, the author also explained the influence of perception concerned with information security threats. This can be deployed to the information security context. The author also emphasized that the perceived likelihood and the negative effect of the threats may cause a perception of health threats that can consequently cause an individual to take protection measures.

[25] Conducted research that emphasized the power of leadership in complying with information security policies. The result of the analysis added that information security education and awareness programs, the severity of the incoming threats, the technical approach in the form of monitoring and policies compliance will increase compliance with information security consciousness. All the studies reviewed looked at employees' and organizations' norms and a few studies have been conducted in respect to the relationship between motivational factors and threats consciousness in respect of students and the University. This incorporates uniqueness into the study as this paper addresses the relationship between motivational factors and threats consciousness among some Malaysian postgraduate students.

II. CONCEPTUAL REVIEW AND HYPOTHESIS

The aims of information security are to safeguard, protect and prevent unauthorized intrusion into the information of the organization. [44] stated that the main objectives of information security and computer security are to ensure data integrity, availability and confidentiality with the cycle of information systems. From the user perspective, [43] stated that if the software is run as it is expected, it could be referred to as a fully secured system.

Information security should cover information security policy, risk analysis, risk management, contingency planning and disaster recovery. With the definition provided, information security is described as a process whereby there is an

information asset accessed, resources and ensuring the availability of the asset whenever there is a need for it. In addition, information security (IS) is controlled in order to provide confidentiality, integrity and availability of an organization's assets [17].

2.1 The relationship between information security awareness and information security threats consciousness

Student awareness in the form of educational training on how to use computers, internet programs and seminars on information security is very important. [37] stated the importance of security awareness perceived by those they surveyed in the year 2007. The computer security survey also analyzed the average respondents and the outcome revealed that the organization was under-investing in security measures at the time the survey was conducted. It gave the assurance that organization knows the crucial issues relating to security awareness [9]. [6] also investigated the impact of information security awareness (ISA) on outcome beliefs. Furthermore, they explored how ISA has significantly affected employees' attitudes towards their organizations' information security rules. Siponen in 2000 proposed a conceptual framework to explain employees' behavior in terms of complying with IS threats. The author incorporates the use of the theory of planned behavior [2]. [6] investigated IS policy compliance and focused on rationality-based beliefs and ISA. They further argued that ISA associates with IS threats. The paper explained that awareness of IS threats is the major key to the IS threat. In conceptualized studies, few studies were conducted in respect of information security threats awareness and its significance amongst students in, which this study will like to address. In this paper, the authors, therefore, propose that

There is a relationship between information security awareness and IS threats consciousness

2.2 The relationship between information security policies and information security threats consciousness

[6] defined information security policy as a guiding statement of a goal to be achieved. [46] agreed with the use of a rules and regulations layout for IS and also stipulated that a penalty will be charged over the information user who refuses to comply with the rules and regulations. The author further stated that so far the policy is in line with the organization's laws; it is expected that such a policy should be able to prevent the information misuse. The absence of an IS policy will make the user not to be aware of the security threats [30] also investigated employees' behavior towards IS threats and observed that attitudes towards complying have a significant impact on threat appraisal and facilitating conditions. [47] and [10] investigated the association between information security threats and organizational policies. The result of the study agreed with our proposed hypothesis that there is an association between an organization's policies and IS threats. We, therefore, hypothesize that:

There is a relationship between IS policies and IS threats consciousness.

2.3 The relationship between perceived threats severity and information security threats consciousness

Threat severity can be traced back to the Protection Motivation Theory (PMT), which explains the information security behavior of individuals. The PMT was developed in 1975 by Rogers as an extension of EVT to provide a more complete understanding of the effects of fear appeals on attitude change [32]. A fear appeal is a communication regarding a threat to an individual that provides information regarding one's well-being [27]. It is used "in persuasive messages to scare people in the hope that the aroused fear will result in the performance of adaptive behaviors" [36]. The severity of the perceived threat is based on prior research showing that the manipulation of fear will affect the perceived magnitude of the threat. [14] examined the effect of IS on individual behavior by adopting PMT to explore individual protection in the use of IS. The study found that threat severity positively supported individual behavior to use the IS. [18] Stated that the perceived threat is determined by two sub-constructs: perceived severity and perceived susceptibility. The results from the study show that there is an insignificant interaction between perceived severity and users of IS. Finally, in a study that examined home users of IS, [9] included direct effects on the perceived threat severity. The result reveals a negative relationship between perceived threat severity and the use of IS. We therefore hypothesized that:

There is a relationship between perceived threats severity and IS threats consciousness.

Conceptual explanation

The conceptual model presented in Fig 1.0 comprises three constructs that are referred to as determinant factors. These factors are hypothesized to have a relationship with the dependent variable (information security threats). The determinant factors are information security awareness, perceived threats severity and information security policies. The authors developed and integrated the protection motivation theory model of information security threats and the theory of planned behaviour to explain the behaviour of the students towards information security threats.

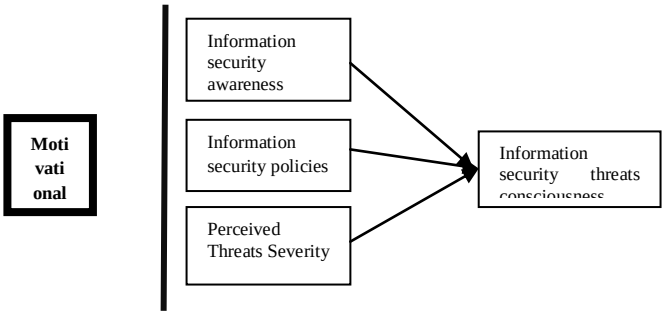

Fig 1.0: Conceptual model of the study

Theoretical background

This study employed the Protection Motivation Theory to explain the concept of information security threats in relation to the determinant factors, which are information security awareness, information security policy, perceived threats severity and information security threats, a deterrence approach.
The PMT explains individual response warnings about threats and any dangerous behaviors, commonly called *fear appeals*. In interpreting and communicating such messages, an individual employs the cognitive process to measure their response towards the threat. It propounds three factors which explain how threats are perceived, termed *threat appraisal factors*. They are rewards or benefits (any intrinsic or extrinsic motivation for increasing or keeping an unwanted behavior); severity (the magnitude of the threat); and vulnerability (the extent to which the individual is perceived to be susceptible to the threat).

PMT equally suggests three factors that explain an individual's ability to cope with the threat, which is called *coping appraisals.* These refer to response to information security policy (the belief in the perceived benefits of the coping action by removing the threat); response cost (to the individual in implementing the protective behavior); and self-efficacy (the degree to which he or she believes it is possible to implement the protective behavior).

[41] Defined perceived severity as the degree to which an individual perceived that the negative consequences caused by BYOD security risks are severe and which have the capability to cause the organization and himself/herself a bad reputation and consequently cause damage to the information of the organization.

This study integrated the information security threats awareness, information security policy and severity of the information security threats to find their relationship with information security threats, with the use of PMT as specified above.

III. RESEARCH METHOD

As discussed above, a quantitative research methodology was employed to achieve the above research objectives and answer the research questions. [8], [42] viewed quantitative research as a study that has quantifiable data. Renowned research methodology theorists like [30] asserted that the most celebrated motives behind using quantitative research are generating conclusions using numbers, establishing people's perceptions and testing for the relationship between the cause and effect variables. [27] Advocate for the quantitative research approach, which he lauds for being explorative enough to extract and deduce the existence of a concept and to generate empirical relationships and influences of the concept. The population used in this study is that of graduate students of the School of Computing and Multimedia, comprising Master's and Ph.D. students. The population comprises University Utara Malaysia postgraduate students who regularly use the internet and who have full knowledge of what information security is about. According to [24], a population of 440 will have a sample size of 205. The Morgan Theory table is used to determine the sampling size of a given population. To ensure the accuracy of the study's

Findings, the researchers made use of 205 as the sample size. When collecting data, 150 of the 205 questionnaires administered were returned.

A questionnaire is a renowned and efficient data gathering quantitative research method [23]. This research used a closed-ended questionnaire to gather data. The questionnaire was adapted from the concept and deductions used to explain the variables in the literature review. It began with a basic introduction to the study, then important objectives of the study and the variables intended to be tested in this study. The information was followed by an assurance to respondents notifying them that their answers are crucial to the study and would only be used for the purpose of the study [4].

3.1 Data analysis

For testing the relationship between the constructs (dependent variable and independent variables), this paper used analysis was done manually using a calculator.). An appropriate descriptive analysis was carried out to give a precise explanation of the research's respondents and how the data have been distributed.

3.2 Respondents' Profile

The gender frequency result distribution below reveals that out of the 150 respondents of the study, 111 are male, and 39 are female. In percentage terms, men constitute 74% and women 24%. It should however be noted that gender is not a significant factor in the issue of information security threats. Table 1.0 below shows the gender frequency distribution.

Table 1.0: Gender

	Frequency	Percent
Male	111	74.0
Female	39	26.0
Total	150	100.0

No	Variable	No. of Item	Pilot Test	Main Test
1	Awareness	5	0.798	0.781
2	Perceive Threat Severity	5	0.745	0.702
3	Compliance to Security Policies	5	0.738	0.703

Table 1.1: Reliability Test

3.3 Reliability Test

Table 1.1 below presents the reliability testing with the pilot testing. After gathering data from the respondents, the reliability test was done using construct reliability. The result was therefore compared with the pilot study by adopting a uniform scale validation in order to determine how consistent the instrument is.

3.4 Result and Discussion

H_1 Information security awareness has a relationship with information security threats consciousness

The hypothesis of the relationship and the influence of awareness of information security threats as elicited in this study use the Pearson product-moment correlation for its testing. A high non-directional (not positive and not negative) correlation between awareness and the information security threat is discovered: The following equation explains the result of the correlation [r—0.791, n-150, p<.05]. It is equally noticed that the 79% variance in awareness could be explained by 79% changes in the information security threats variable. With the significance less than 0.05, it shows that the tested hypothesis is accepted. The result in Table 1.2 below shows the degree of the relationship, which has positively answered the question*: What is the relationship between awareness and information security threats?*

Table 1.2: Correlation result for Hypothesis 1

		Information Security Threats
Information security Awareness	Pearson Correlation	.791**
	Sig. (2-tailed)	.000
	N	150

**Correlation is significant at the 0.01 level (2-tailed).

H_2 Compliance *with security policies has a relationship with information security threats*

The second hypothesis of the study is also tested the Pearson product-moment correlation. The result of the correlation is presented showing that there is a correlation between compliance with security policies and information security threats. With the equation below, explanation on it can also be stressed using the following correlation equation: [r—0.751, n-150, p<0.05].

Its shows that 75% variances in compliance with security policies explain 75% variances in the relations with the information security threats variable. The result has answered the second question of the study: What is the relationship between compliance with security policies and information security threats?

Table 1.3: Correlation result for Hypothesis 2

		Information security threats consciousness
Compliance to information security policies	Pearson Correlation	751**
	Sig. (2-tailed)	.000
	N	150

H_3 ***Perceived threats severity has relationship with information security threats consciousness.***

The third hypothesis of this study is equally tested with Pearson product-moment correlation, and the result of the correlation is presented in Table 1.4 below. The result reveals that there is a correlation coefficient between perceived threats severity as a variable, and speaking anxiety. The result is further explained with the following correlation equation [r—0.741, n-150, p<0.05].

It shows that 74% variances in perceived threats severity is explainable by 74% variances in its relations with information security threats. The research question that - What is the relationship between perceived threats, severity and information security threats? - is thus answered.

Table 1.4: Correlation result for Hypothesis 3

		Information security threats consciousness
Perceived threats severity	Pearson Correlation	741**
	Sig. (2-tailed)	.000
	N	150

IV. DISCUSSION

This paper did not consider the relationship between respondents' demographics and information security consciousness as this is not important to this study. Therefore, they were not discussed in detail. More so, respondents' demographics are not considered as principal factors in determining the relationship that exists between the independent variables and dependent variable. Below are explanations on the descriptive analysis of the study which explores the relationship between the determinant factors and information security threats.

4.1 Information security awareness associates with information security threats

This study has agreed with the findings that awareness associates with information security threats. It agrees with [31] whose empirical findings suggested that training and education are related with information security threats and the content of the awareness are training, education and compliance with the policies of the organization. [45] Investigated information security threats, taking perceived threats, policy compliance and awareness of information severity threats as determinant factors. The result of the study complied with the hypothesis that there is an association between awareness and information security threats. In the same vein, [19] suggested that the severity of punishment has a negative influence on the security habit of compliance. This suggested that it is better to apply awareness than the severity of punishment. [38] agreed that in combating information security threats, awareness in the form of training must be considered. The author emphasized that awareness has a significant effect on information security threats. [38] presents the Deterrence Model to explain control that causes the misuse of information systems. The model specified that awareness of the user in information security countermeasures significantly influenced the perceived certainty and severity of organizational sanctions associated with IS misuse, which leads to reduced IS misuse intention. Therefore, the literature review shows that a relationship exists between information security awareness and information security threats as hypothesized above.

4.2 Compliance with information security policies has relationship with information security threats consciousness

Presently, many organizations recognize how important compliance with the information security policies (ISP) of their respective organizations is. [36] carried out an empirical

investigation on information security policies compliance by employees. The author identified compliance with information security policies of the organization as an act of necessity as the author investigated rationality-based factors that motivate the employees to comply with information security policies. The result of the investigation revealed that employees' intention to comply with information security policies has a significant relationship with the motivational factors, which are normative beliefs and self-efficacy. In the same breath, these inversely reduce information security threats. The key threat to information security is non-compliance with information security policies.

[37] developed the Multi_theory Model to explain user compliance with the rules and regulations guiding the use of the information and assets of the organization. They combined elements from the Protection Motivation Theory, the Theory of Reason Action and the Cognitive Theory. The model was validated using SEM-base. The outcome of the analysis reveals that the perceived severity of potential information security threats, employees' beliefs, perceived vulnerability to potential security threats, employees' attitudes pertaining to ISSP and social norms had a significant and positive effect on employees' intention to comply with information security policies, as the compliance to policy reduces information security threats. [37] This study supported the current study as it explained the importance of information security compliance because when the compliance with information security policies is being carried out, the inverse effect is being felt in the reduction in information security threats, as the authors have rightly hypothesized.

[13] agreed with the finding that information security compliance associates with information security threats. Although the compliance with information security policies was not studied in isolation, it has a direct link with perceived severity which affects information security threats. They studied policy compliance and its association with information security threats. A lack of security awareness can make an organization's information vulnerable to these internal and external threats. Information security threats consciousness come into play when users are aware and educated about the incoming threats and how vulnerable their information is if the proactive action to secure it is not taken. Threats conscious can be information education or training to make the computer user aware of the impending danger if the information of such an organization or an individual is not protected [11].

4.3 Perceived threats severity has a relationship with information security threats consciousness

The empirical results of this study revealed that perceived information security threats are associated with information security threats. As suggested by [19], the deterrent severity has no association with a proactive use of information systems, but the preventive effort has a role to play in the proactive use of information system security. However, [11] suggested that awareness of information security countermeasures has an effect on perceived severity and the certainty of that punishment that comes with information security.

[34] perceived severity is the perception that an individual has about the seriousness of information security threats and explains how that seriousness could allow a change in individual's behavior. The study carried out by [34] to investigate the seriousness of information security threat amongst students agreed with that information. Results specified that the perceived severity of threats could cause information threats consciousness in the user. The result is in line with this study.

A study conducted by [28] suggests that perceived threat vulnerability and perceived threat severity affect attitudes towards information security threats and also have a positive association with the perception of information security threats.

The result of the study is in line with the current analysis results that have proposed that perceived threats severity has a relationship with information security threats. [34] Identified the importance of the severity of information security threats in complying with information security in an organization. They employ one element of the Theory of Planned Behavior to explain adherence of employees to information security policy. They proposed that information security threat severity has a significant effect on employees' intention to comply with ISP.

The result of the analysis explained that the severity of information security threats has a significant effect on information security compliance, which in turn has an effect on information security threats. [23] explains that perceptions pertaining to the severity of the threats and the efficacy of the response may possibly have a positive influence on the information security threats consciousness, which in turn may have a positive influence on policy compliance. All the authors in this section are in conformity with this study's result. Therefore, it is in line as hypothesized above.

4.4 Implications of the study

The implications of the study cut across both practical and theoretical aspects of information security motivational factors. From the results, the awareness of information security is found to have an association with information security. This indicates how indispensable awareness is to information security. University management is employed to educate and train students on security in relation to their information and data. Training should also emphasize the importance of the information security policy to university information security,

as well as compliance with the policies during the training period. The management is expected to write the policies clearly and post them where the students can easily see. As seen in the results of this study, information security policies have a relationship with information security threats. As such, compliance with information security policies by university management and students should be taken seriously. The results also revealed that the perceived severity of information security threats is associated with information security threats. Information of the students and management data are very important to the university. These are assets that should be taken care of. During training, students are expected to know how severe the threats are to their personal information. This will make them guard it jealously.

V. CONCLUSION

Starting from the literature reviewed, data analysis and the findings from the hypotheses tested, this study agrees that each of the independent variables: awareness of information security threats, perceived threats severity and compliance with information security has a relationship with the dependent variable, which is information security threats. So far, this study has added to previous studies on information security issues. Equally the study also gives strength to those past studies that have similar findings on information security relations and motivational factors. In conclusion, this study has submitted empirical results that show the empirical relationship between motivational factors and information security threats amongst the students.

Recommendation

This study was carried out with students in a University. It was constrained by time and a lack of resources. Other researchers can consider extending the scope of the study by considering other organizations, like banking sectors, communications companies, information technology companies, hospitals and generally where information security threats are prominent. Besides this, this study employed quantitative methods to carry out the study. Other researchers can employ mixed methods for their analysis to be based on large volumes of data. Furthermore, this research is based on three constructs to measure the relationship between the dependent and independent variables, but other researchers can use more constructs.

Acknowledgement

The authors will like to acknowledge the anonymous reviewers for their valuable comments.

REFERENCES

[1] A. Albuquerque Junior and E. Santos, "Adoption of Information Security measures in public research institutes", *Journal of Information Systems and Technology Management*, vol. 12, no. 2, 2015.

[2] E. Albrechtsen and J. Hovden, "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study", *Computers & Security*, vol. 29, no. 4, pp. 432-445, 2010.

[3] T. Finne, "A conceptual framework for information security management", *Computers & Security*, vol. 17, no. 4, pp. 303-307, 1998.

[4] B. Ali, "Is it possible for qualitative research to be properly valid and reliable", *The University of Warwick*, vol. 1-19, p. 7, 2012. [Accessed 16 May 2019].

[5] R. Baskerville and M. Siponen, "An information security meta- policy for emergent organizations", *Logistics Information Management*, vol. 15, no. 56, pp. 337-346, 2002.

[6] Bulgurcu, Cavusoglu and Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness", *MIS Quarterly*, vol. 34, no. 3, p. 523, 2010.

[7] R. Plotnikoff and L. Trinh, "Protection Motivation Theory", *Exercise and Sport Sciences Reviews*, vol. 38, no. 2, pp. 91-98, 2010.

[8] M. Ishtiaq, "Book Review Creswell, J. W. (2014). Research Design: Qualitative, Quantitative and Mixed Methods Approaches (4th ed.). Thousand Oaks, CA: Sage", *English Language Teaching*, vol. 12, no. 5, p. 40, 2019.

[10] C.L. Anderson, R. Agarwal, Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions, *MIS quarterly*, vol.*34*,no.3,pp 613-643,2010.

[11] Chen CC, Shaw RS, Yang SC. Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system. Information Technology, Learning & Performance Journal vol.24, no1,pp1-14 2006.

[12] H. Bojmaeh, "Mediating role of Information System Security Awareness in the relationship between Self-Efficacy, Security Practice and Information System Security Behavior", *International Journal of Science and Engineering Applications*, vol. 4, no. 6, pp. 361-365, 2015..*Computer Engineering*, 13.

[13] J. D'Arcy, A. Hovav and D. Galletta, "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach", *Information Systems Research*, vol. 20, no. 1, pp. 79-98, 2009.

[14] D. Dang-Pham, S. Pittayachawan and V. Bruno, "Exploring behavioral information security networks in an organizational context: An empirical case study", *Journal of Information Security and Applications*, vol. 34, pp. 46-62, 2017.

[15] S. Dzazali and A. Hussein Zolait, "Assessment of information security maturity", *Journal of Systems and Information Technology*, vol. 14, no. 1, pp. 23-57, 2012.

[16] K. Guo, Y. Yuan, N. Archer and C. Connelly, "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model", *Journal of Management Information Systems*, vol. 28, no. 2, pp. 203-236, 2011.

[17] C. Gikas, "A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards", *Information Security Journal: A Global Perspective*, vol. 19, no. 3, pp. 132-141, 2010.

[18] A. E. Howe, I. Ray, M. Roberts, M. Urbanska, & Z. Byrne, *The psychology of security for the home computer user.* Paper presented at the Security and Privacy (SP), 2012 IEEE Symposium on.

[19] T. Herath and H. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness", *Decision Support Systems*, vol. 47, no. 2, pp. 154-165, 2009.

[20] P. Ifinedo, "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition", *Information & Management*, vol. 51, no. 1, pp. 69-79, 2014. Available: 10.1016/j.im.2013.10.001.

[21] K. Alshare, P. Lane and M. Lane, "Information security policy compliance: a higher education case study", *Information and Computer Security*, vol. 26, no. 1, pp. 91-108, 2018.

[22] R. Klein and E. Luciano, "What Influences Information Security Behavior? A Study with Brazilian Users", *Journal of Information Systems and Technology Management*, vol. 13, no. 3, 2016.

[23] K., Khalid H., Abdullah & M, D Kumar.Get along with quantitative research process. *International Journal of Research in Managemen,vol.2,no.2,* pp.15-29,2012.

[24] R. Krejcie and D. Morgan, "Determining Sample Size for Research Activities", *Educational and Psychological Measurement*, vol. 30, no. 3, pp. 607-610, 1970..

[25] H. Kim, H. Choi and J. Han, "Leader power and employees' information security policy compliance", *Security Journal*, 2019. Available: 10.1057/s41284-019-00168-8.

[26] K. Hausken, "A Strategic Analysis of Information Sharing Among Cyber Attackers", *Journal of Information Systems and Technology Management*, vol. 12, no. 2,pp. 245-270. 2015.

[27] R. Kumar, S. Park and C. Subramaniam, "Understanding the Value of Countermeasure Portfolios in Information Systems Security", *Journal of Management Information Systems*, vol. 25, no. 2, pp. 241-280, 2008.

[28] H. Liang and Y. Xue, "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective", *Journal of the Association for Information Systems*, vol. 11, no. 07, pp. 394-413, 2010.

[29] S. Milne, P. Sheeran and S. Orbell, "Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory", *Journal of Applied Social Psychology*, vol. 30, no. 1, pp. 106-143, 2000.

[30] M. Siponen, M. Adam Mahmood and S. Pahnila, "Employees' adherence to information security policies: An exploratory field study", *Information & Management*, vol. 51, no. 2, pp. 217-224, 2014.

[31] Computer crime survey", *Computer Fraud & Security Bulletin*, vol. 7, no. 12, pp. 1-4, 1985.

[32] R. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change1", *The Journal of Psychology*, vol. 91, no. 1, pp. 93-114, 1975..

[33] D. Roskos- Ewoldsen, J. Yu and N. Rhodes, "Fear appeal messages affect accessibility of attitudes toward the threat and adaptive behaviors", *Communication Monographs*, vol. 71, no. 1, pp. 49-69, 2004.

[34] L. Muniandy, B. Muniandy and Z. Samsudin, "Cyber Security Behaviour among Higher Education Students in Malaysia", *Journal of Information Assurance & Cybersecurity*, pp. 1-13, 2017.

[35] J. Shropshire, M. Warkentin and S. Sharma, "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior", *Computers & Security*, vol. 49, pp. 177-191, 2015.

[36] M. Siponen, "A conceptual foundation for organizational information security awareness", *Information Management & Computer Security*, vol. 8, no. 1, pp. 31-41, 2000.

[37] M. Siponen, M. Adam Mahmood and S. Pahnila, "Employees' adherence to information security policies: An exploratory field study", *Information & Management*, vol. 51, no. 2, pp. 217-224, 2014.

[38] R. Shaw, C. Chen, A. Harris and H. Huang, "The impact of information richness on information security awareness training effectiveness", *Computers & Education*, vol. 52, no. 1, pp. 92-100, 2009.

[39] M. Tribus, "Quality in R&D: Applying Quality Management Principles", *Research Management*, vol. 30, no. 6, pp. 11-21, 1987

[40] J. Shropshire, M. Warkentin and S. Sharma, "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior", *Computers & Security*, vol. 49, pp. 177-191, 2015.

[41] T D. Dang-Pham and S. Pittayachawan, "Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach", *Computers & Security*, vol. 48, pp. 281-297, 2015.

[42] I. Newman and D. Newman, "Media Review: Thomas, R. Murray. (2003). Blending Qualitative and Quantitative Research Methods in Theses and Dissertations. Thousand Oaks, CA: Corwin Press", *Journal of Mixed Methods Research*, vol. 1, no. 3, pp. 295-297, 2007.

[43] R. von Solms, "Information security management: why standards are important", *Information Management & Computer Security*, vol. 7, no. 1, pp. 50-58, 1999. Available: 10.1108/09685229910255223.

[44] C. Vroom and R. von Solms, "Towards information security behavioural compliance", *Computers & Security*, vol. 23, no. 3, pp. 191-198, 2004.

[45] M. Yesilyurt, & Y .Yalman, Security Threats on Mobile Devices and their Effects: Estimations for the Future. (2016) *Int. J. Secur. Its Appl.*, *10*(2), 13-26.

[46] M. Whitman, "In defense of the realm: understanding the threats to information security", *International Journal of Information Management*, vol. 24, no. 1, pp. 43-57, 2004.

[47] W. Adedayo and S. Ayobami, "Relationship between Information Security Awareness and Information Security Threat.", *Threat. International Journal of Research in Commerce, IT & Management,*, vol. 3, no. 8, p. 7, 2019. [Accessed 27 May 2019].

APPENDIX

I am currently conducting a research on information security among the UUM community the result of this study will e interested in your experiences concerning information security issue, therefore enclosed questi01maire which am exp Information security. Your participation will be highly appreciated.

Thanks.

Sincerely,

Williams Adedayo Solomon,

(MSC IN ICT).

Section A

Demographic section

Male

Female

Indicate your agreement with the following statements:

Section B **Information security threats severity**		**Strongly Disagree**	**Disagree**	**Slightly Disagree**	**Neutral**	**Slightly Agree**	**Agree**	**Strongly Agree**
01	an information security breach in my UUM will be a serious problems to me							
02	information security are becoming more serious every daily basis in UUM							
03	An information security breach in my organization would be a serious problem for my organization							
04	Losing University information as due to opening a suspicious email attachment is a serious problem for me.							

04	**Losing University information as due to opening a suspicious email attachment is a serious problem for me.**							
05	If the information inside my computer is infected by malware due to opening a suspicious email attachment, may cause a serious damage to my work							
	Section C **Information security threats awareness**							
01	I am aware of impending security threats and breaches if I do not close UUM web when after used							
02	I was thought the security threats issues at my first year							
03	I am aware that leaving my school email opened after used can cause serious damage to my information							
04	I am not aware of any issue regarding information breaches							

05	The management slightly alerts us when there is an information breaches.							
01	**Section D** **Information security policies compliance**							
O2	I always comply with the rules guiding information security in UUM							
03	It is not necessary for me to close the learning zone and my portal after accessing it							
04	I am not under obligation to comply to any information security in UUM							
05	I sometime do obey the rules and regulation regarding information security in UUM							
5	I do feel boring to close portal and learning zone after researching for an information							