Asian Journal of Computer Science and Technology
ISSN: 2249-0701 Vol.8 No.2, 2019, pp. 77-84

Information Security Awareness among Non-Academic Staff in the University of Ibadan, Nigeria

H. T. AbdulRahman[1] and S. O. Oladipupo[2]
[1&2]Africa Regional Centre for Information Science, University of Ibadan, Ibadan, Nigeria
E-Mail: hafsatrahman19@gmail.com, samladoluy2k5@yahoo.co.uk

Abstract **- This study applied the established factors from the existing literatures on information security awareness to investigate information security awareness among non-academic staff in the University of Ibadan, Nigeria. The objectives of this study are; to identify the factors that influence information security awareness and to determine the level of information security awareness among non-academic staff. This study employed a survey design. Stratified random sampling technique was utilised to select the respondents for the study. The study participants consist of non-academic staff in the University of Ibadan. A field survey of 300 respondents was carried out using questionnaire as the main instrument. Descriptive statistics was used for data analysis. Findings of this study revealed that information security awareness is significantly influenced by policy of information security, education of information security, knowledge of technology, and non-academic staff's behaviour. Furthermore, findings show that the level of information security awareness among non-academic staff in the University of Ibadan was high. Finally, findings were discussed and recommendations for the future research were also addressed.**
Keywords: **Information Security, Awareness, Non-Academic Staff, University of Ibadan, Nigeria**

I. INTRODUCTION

First generation of computers introduced into organisations, took the form of standalone mainframe computers with single processors (Solms, 1998). These mainframe systems did not support the use of databases and only supported one user working on them at a time. These users were limited to dedicated computer personnel trained in the secure use of such systems (Thomson, 1998). In order to ensure that only these users were allowed access, physical controls such as locking doors were implemented and proved to be adequate protection. The multi-user era was brought on by the introduction of computers that could perform multi-processing and allow multiple users to log on simultaneously. Workstations for users were now provided in their working environment and became part of their daily functions. Resources, like memory and databases were now shared and could be accessed remotely in a distributed form (Thomson, 1998). This brought the problem of ensuring that only authorised users gained access to these resources. To ensure this, technical controls such as authentication and access control were necessary.

Presently, lots of organisations are interconnected through their Information Technology (IT) systems, for an easier and faster sharing of data for work, study, and communications, and many other routine human tasks. This may result in an information security risk for an organisation (Solms, 1998). Any interruption of information security may kill the main purpose of this sophisticated technology, hinder the smooth operation of an organisation, make users feel doubtful and shocked, and could cause losses to the organisations involved. According to Segev, Porra and Roldan(1998), in order to attain security, utilising technology is not enough but rather the organisation itself does matter. Besides, it should be noted that information system security is at both organisational and technical level, as well as its implementation has to have cognizance of both human and ethical considerations (Trompeter and Eloff (2001). Hinde (2003) stated that carelessness towards privacy could cause an organisation to have a big financial loss. Most of the studies on information security are technical in nature and have limited emphasise on organisational and individual. Today, many organisations do not have enough consideration on individual value and so they just draw attention to technical aspects. Because of technical failures and human errors, organisations need to be conscious about necessity of educating answerable employees in order to strengthen information system security. This leads to another aspect of the information security, known as information security awareness.

Regarding the University setting, the conventional method for managing the increased volume of information is insufficient. At present, the University has switched to an electronic-based system. ENISA (2006) affirmed that organisations, whether private or public, are gradually storing and making information available by electronic means, and therefore, there is an increase in the dependence on IT systems. This study has chosen non-academic staff in the University of Ibadan, Nigeria as the study scope. It implies that this study seeks to understand the key influential factors influencing awareness of information security among non-academic staff in the University of Ibadan.

II. OBJECTIVES OF THE STUDY

The general objective of this study is to evaluate information security awareness among non-academic staff in the University of Ibadan, Nigeria while the specific objectives are to:

1. To identify the factors that influence information security awareness.

2. To investigate the level of information security awareness among non-academic staff in the University of Ibadan.

III. RESEARCH QUESTIONS

The study has been conducted to answer the following research questions.
RQ1: To what extent do policy of information security influences information security awareness?
RQ2: To what extent do education of information security influences information security awareness?
RQ3: To what extent do knowledge of technology influences information security awareness?
RQ4: To what extent do employee's behaviour influences information security awareness?

IV. LITERATURE REVIEW

A significant body of literature exists in the area of information security at national and international level. The emphasis has been given in this section to review the literature published in various reputed journal articles. Regardless of computer security, humans are still the main factor involved in errors, faults, misleading, and many other damages or losses of information in computer systems (NurulHidayah, 2009). Notwithstanding, proper implementation of security technology, the same issues are still arising in security attacks, such as social engineering, dishonesty, and negligence. Security problems nowadays are mostly caused by the inadequate security awareness of the users (Chen, Shaw, and Yang, 2006). Zahri and Ahmad Nasir (2003) stated that countries that use a lot of ICT, especially the internet, are vulnerable to cyber-attacks. Information systems are widely used nowadays. A lot of information is being processed, stored, transferred, and manipulated for business purposes. Organisations particularly need to secure their information, and often put into practice security measures by placing security devices and software into their IT and network equipment, such as antivirus, firewalls, monitor network traffic, and many more. However, notwithstanding the sophisticated equipment and software used, without an awareness of the importance of information security, the company's information and knowledge may fall into the hands of deceitful people or organisations. Caroll (2006) noted threats coming from inside of an organisation are more difficult to trace, because there is no way to monitor a person's actions or intention.

According to Boyce and Jennings (2002), security awareness occurs when a user understands the security policies, procedures, and practices, so as to make sound judgments when a potential security issue occurs, in the absence of further directive. The aim of information security awareness is to improve information security by enhancing and adopting security policies and countermeasures (ENISA, 2006), improving IS users' security behaviour (Puhakainen, 2006), or altering work routines, so that good security habits are applied (Hansche, 2001). The importance of information in an organisation, sometimes called intangible assets, plays a key role to the drivers and technology used as a key enabler (Shashi, 2007). The objective of awareness is to minimise human related faults (Siponen, 2000). Several authors affirm that the motive of information security awareness is to define that term. It is refer to the extent to which every member of staff understands, the importance of information security, the levels of information security appropriate to the organisation, their individual security responsibilities and acts accordingly (Mathisen, 2004). Maeyer (2007) defines security awareness as an organised and ongoing effort to guide the behaviour and culture of an organisation in regard to security issues. For instance, it implies that a company wants to secure its confidential information from its opponents. Therefore, employees must not disclose particular information to their competitors; if not, the awareness level among staff in that company is not as good as their mission. Apparently, information security awareness can bring many benefits to an organisation. However, the return on investment for an awareness program should not be looked at merely from a dollars and cents point of view. Due to the rapid growth of the internet, fundamental information security needs to also grow. Moreover, when a company is connected to the internet, any user in cyberspace can have access to its website. Accordingly, while many tactics provide an assurance of protection, carelessness can also be a key factor. Alternatively, awareness training and education should be used to remind staff that an internet security breach could have a profound effect on the health of the organisation, and hence, their job security (Everet, 1998). This is one of the situations that could clarify why information security awareness is essential. More upsetting, is the existence of those that are self-satisfied and ignore the issue of information security, until their behaviour leads to information leakage. Either intentionally or accidentally, information leaks can harm an organisation. Solms (1998) pointed out that the aim of information security is to ensure business continuity and to minimise business damage, by preventing and minimising the impact of security incidents. Information protection usually depends on an information security plan and management, which involves humans (Kruger, Drevin, and Styen, 2010). This signifies that knowledge, education, and awareness, plays a significant role in the success of information security, to protect organisational information. For instance, when an employee does not logoff from a computer after use, deceitful people can steal data from the computer and use it for personal gain or to compete with that particular organisation. Hence, this is the consequence of a behaviour that does not understand the importance of information security awareness.

V. THEORETICAL FRAMEWORK

In accordance with the literature reviewed, it can be deduced that the four key factors are closely associated with information security awareness. These factors include policy of information security, education of information

security, knowledge of technology, and human behaviour in the working environment. Having these factors in place, it can be said that a particular organisation has reached an acceptable level of information security awareness. Policy is a guideline to an organisation regarding information security. Martins and Eloff (2003) stated that guidelines and instructions of awareness are important aspects of maintaining stability. Solms and Solms (2004) opined that policies should provide guidance to employees and partners, to how they should act and behave in order to be in line with management's wishes. With clear guidelines in place, IS can strengthen the information security efforts (Straub, 1990). Haeussinger and Kranz (2013) study revealed provision of security policies as one of the most influential antecedents of ISA. In terms of education, Thomas (2005) noted that an effective information security program cannot be implemented without implementing employee awareness and training program to address policy, procedures, and tools. Many companies place good security devices in their organisation. Adequate information security training is required to create and improve user awareness and behaviour towards information security within the organisation (Albrechtsen and Hovden, 2010). A study by Straub and Welke (1998) focusing on educating organisational management established that implementing a security awareness training program could help to reduce system risks. Yngström and Björck (1999) argue that ISA is a component of an information security training and education program. Takemura (2010) suggested the necessity for enhancing information security education, in order to motivate Japanese workers' awareness of information security. This notion was supported by other researchers such as Oladipupo (2019), Fakeh, Zulhemay, Shahibi, Ali, and Zaini (2012), D'Arcy, Hovav, and Galletta (2009), and Kruger *et al.,* (2010).

As regards knowledge of technology, recently, most work in organisations has come to depend on information technology to operate, such as managing records, business transactions, and communicating with others. Technology facilitates day-to-day activities or operations, but can also cause harm, if adequate care is not taken. For example, weak passwords can cause a loss of data in records, trust in internet fraud, such as spam, phishing, and social engineering, and could lead to customers being cheated. Hence, knowledge of technology is imperative and applicable to the issue of information security. Flinn and Lumsden (2005) established knowledge of specific technologies that relate to their security and privacy when using the internet can prevent harm from happening. Haeussinger and Kranz (2013) in their study also revealed employees' knowledge on information systems as one of the most influential antecedents of ISA. Sole limitation of an organisation, which impacts the effectiveness of technologies, is the behaviour of the human beings that administer, use, access, and maintain, information resources (Solms and Solms, 2004; Vroom and Solms, 2004). According to Kruger and Kearney (2006), human behaviour consists of an intention to act in a particular manner. Also, Thomson and Solms (1998) discussed about changing human interest for information security awareness program, by using psychological principles that have been ignored by information security practices. Similarly, Gordon (2010) directly determined the relationship between security awareness and security behaviour in individuals. In the same vein, Kaur and Mustafa (2013) established a significant relationship between behaviour and information security awareness. Besides, sustaining a positive security-behaviour is a key factor in an effective information security environment. The conceptual framework of this study is illustrated inFig.1.

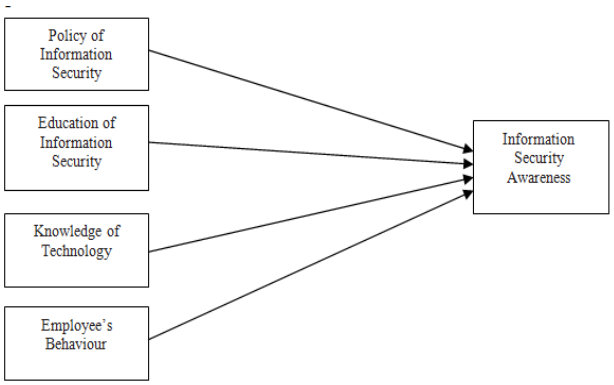

Fig.1 Conceptual Framework

The four factors shown in Fig.1 were selected by analysis of prevailing factors that influence information security with respect to awareness. These factors are the main points of understanding, obtained from the previous articles, research, and dissertations of numerous authors. The framework shows relationships between the independent variables and dependent variable. The framework posits that the policy of information security, education of information security, knowledge of technology and employees' behaviour could have influence on information security awareness. As discussed, policy is a reference for employees. It is a tool for management to guide their subordinates, by educating them based on what the policy states. Education is a communication between user and educator. Education can influence the knowledge of the end user. Knowledge of technology is important, as information is organised and communicated using technology. Knowledge can change human behaviour. By having knowledge, users can act appropriately. They know how to act when something occurs, by making the right decision for a situation, and in a time that can avoid unsuitable events in the place of work. For example, an employee must not click any link sent to them, because he/she feels insecure about that link. Alternatively, if the link appears frequently, he/she can refer to IT department for further information.

Two right behaviours in this situation are (1) he/she did not click the undefined link, and (2) he/she refers to IT department before ignoring or proceeding to the next action. Both show that he/she is aware of the insecure environment around him/her and he/she knew of the risk if the link was bad.

VI. METHODOLOGY

This study was conducted by structured questionnaire survey to gather the data. This study also adopted a cross sectional research design for data collection purpose. This study used questionnaires from the previous research (Fakeh, *et al.,* 2012) and makes an alteration to adapt with research objectives. The questionnaire of this study comprised two main parts and took approximately 10 to 15 minutes to be completed. The first part of the questionnaire consists of the demographical characteristics of the respondents. It includes gender, age, educational qualification, faculty, and years of experience. The second part called as information security awareness and sought to measure the information security awareness in the context of non-academic staff. This part was further divided into five sections: policy of information security (PIS), education of information security (EIS), knowledge of information technology (KIT), employee's behaviour (EB), and information security awareness (ISA). The questionnaires have 26 questions represented five (5) variables using a scale of one (No), two (Don't know), three (Yes). This scale applied for all the questions in part B.

Despite the fact that the variables in the survey instrument were adapted from prior studies where they have been tested and validated, they have not been validated in the context of non-academic staff, especially in the University of Ibadan. Hence, a pilot study was conducted to assess the adequacy of the questionnaire. Twenty-five questionnaires were administered for the pilot study. Data collected from the pilot study were used to perform item analysis to preliminarily assess the internal consistency of constructs. The pilot study led to further modifications after the questionnaire went through a face validity test by an expert in the field of study. The result of the reliability test shows that all variables have good or excellent internal consistency.

Abridged versions of questionnaire were administered by the researchers to non-academic staff in the University of Ibadan. Stratified random sampling method was done to collect the data from samples, which represent all the populations' characteristics. The collection of data was carried out within ten weeks, and the unit of analysis in this study was individual unit. In this study, the non-academic staff in the university formed the unit of analysis. The population of non-academic staff in the University of Ibadan as at June 2017 was 4113 according to the information sourced from the Bursary Department and Finance Office, University of Ibadan. A total of 411 questionnaires were randomly distributed to thirteen faculties in the university, out of which only 300 (73.0%) questionnaires was collected and were considered suitable for analysis. The duly completed questionnaires were statistically analysed using SPSS for Windows (20.0 Version). The analysis of data was done using frequency count, percentages, mean and standard deviation. The data presented in Table I represent the demographic characteristics of the respondents.

VII. ANALYSIS AND RESULTS

A. Demographic Characteristics of the Respondents

TABLE I DEMOGRAPHIC CHARACTERISTICS OF THE RESPONDENTS

Demographic characteristics of the Respondents (n= 300)		**Counts**	**Percentage (%)**
Faculty	Central Administration	175	58.3
	Basic Medical	12	4.0
	Clinical Science	10	3.3
	Dentistry	6	2.0
	Infection and Diseases	2	0.7
	Agriculture	12	4.0
	Arts	14	4.7
	DLC	5	1.7
	Education	15	5.0
	Law	2	0.7
	Pharmacy	4	1.3
	Science	21	7.0
	Social Science	22	7.3
Gender	Male	179	59.7
	Female	121	40.3
Age	21 – 30 years	20	6.7
	31 – 40 years	95	31.7
	41 – 50 years	117	39.0
	51 – 60 years	62	20.7
	61 – 70 years	6	2.0
Educational Qualification	ND	80	26.7
	NCE	16	5.3
	HND	69	23.0
	B.Sc/B. Ed/B.A	85	28.3
	Masters/PGD	47	15.7
	M. Phil	2	0.7
	Ph.D	1	0.3
Years of Experience	1 – 5 years	25	8.3
	6 – 10 years	75	25.0
	11– 15 years	73	24.3
	16 – 20 years	49	16.3
	21 – 25 years	43	14.3
	26 – 30 years	16	5.3
	Over 30 years	19	6.3

As presented in Table I, 175(58.3%) of the respondents were in Central Administration, while 2(0.7%) was in Faculty of Law and Infection & Diseases. The study also revealed that males dominantly made up 179(59.7%) of the respondents, while 121(40.3%) of the respondents were females. Majority of the respondents 117(39.0%) fell within the age group of 41-50 years, while the least proportion of the respondents 6(2.0%) fell within the age group of 61-70

years. Furthermore, respondents with Ph.D. degree accounted for 1(0.3%), 2(0.7%) had Master of Philosophy (M.Phil.) degree, 47(15.7%) had Masters/PGDE degree, 85(28.3%) had Bachelor of Science/Education/Arts (B.Sc. /B.Ed. /B.A.) degree, 69(23.0%) had Higher National Diploma (HND) degree, 16(5.3%) had Nigeria Certificate in Education (NCE) and 80(26.7%) had National Diploma (ND). Lastly, 19(6.3%) of the respondents had practiced for more than 30 years, 16(5.3%) had practiced for between 26 and 30 years, 43(14.3%) for between 21 and 25years, 49(16.3%) for between 16 and 20 years, 73(24.3%) for between 11 and 15 years, 75(25.0%) for between 6 and 10 years and 25(8.3%) of the respondents had practiced for less than 6 years.

B. Answering the Formulated Research Questions

1) Research Question 1: What are the influences of policy of information security on information security awareness among non-academic staff?

C. Policy of Information Security

Table II discussed the influence of policy of information security on information security awareness. The results revealed that 226 (75.3%) of the respondents claimed that they have security team in place in the academic institution, 69(23.0 %) were not sure, and 5(1.7%) said no. Moreover, 237(79.0%) of the respondents admitted that their computers were configured to automatically update, 43(14.3%) did not know, and the rest 20(6.7%) said no.

In the same vein, majority of the respondents 256(85.3%) knew who to contact if their computers is hacked or infected, 31(10.3%) were not sure, while only 13(4.3 %) said no. Similarly, in terms of guidelines regarding information security in the respondent's workplace, 205(68.3%) answered yes, while 51(17.0%) were not sure, and the rest 44(14.7%) said no.

TABLE II EXTENT OF THE INFLUENCES OF POLICY OF INFORMATION SECURITY ON INFORMATION SECURITY AWARENESS

Policy of Information security	No	Don't Know	Yes	Mean	Standard Deviation	Rank
We have a information security team in this organisation	5(1.7%)	69(23.0%)	226(75.3%)	2.213	0.449	1
My computer is configured to automatically update	20(6.7%)	43(14.3%)	237(79.0%)	2.077	0.453	2
I know who to contact if my computer is hacked or infected	13(4.3%)	31(10.3%)	256(85.3%)	2.060	0.379	3
There are guidelines regarding information security in my workplace	44(14.7%)	51(17.0%)	205(68.3%)	2.023	0.563	4
There are policies on which websites I am allowed to visit	48(16.0%)	52(17.3%)	200(66.7%)	2.013	0.578	5
The firewall on my computer is always enabled	38(12.7%)	22(7.3%)	240(80.0%)	1.947	0.445	6

Furthermore, 200(66.7%) of the respondents claimed they had policies on which websites they were allowed to visit, 48(16.0%) said no, and the rest 52(17.3%) were not sure. Besides, majority of the respondents 240(80.0%) kept the firewall on their computer on, 38(12.7%) said no, while only 22(7.3%) were not sure. Conclusively, results reveal that the most significant item fell under the existence of a security team in the organisation (μ=2.213). My computer is configured to automatically update ranked second, and the firewall on my computer is always enabled ranked last.

2. Research Question 2: What are the influences of education of information security on information security awareness among non-academic staff?

D. Education of Information Security

Table III examined the influence of education of information security on information security awareness. Results reveal that 93(31.0%) of the respondents do not know the value of their computer to hackers, 152(50.7%) answered yes, and 55(18.3%) said no. Also, 244(81.3%) of the respondents knew what to do if their computer is infected with a virus, 32(10.7%) said no, while 24(8.0%) do not know. In the same vein, 196(65.3%) of the respondents claimed that they knew what a phishing attack was, while 60(20.0%) said no, and the rest 44(14.7%) were not sure.

Likewise, majority of the respondents 144(48.0%) agreed that they received training on information security in their workplace, 36(12.0%) claimed that they don't know, and the rest 120(40.0%) said no. Besides, 158(52.7%) of the respondents affirmed that they had experienced virus or trojan on their computer, 114(38.0%) said they never found a virus, and 28(9.3%) admitted that they do not know. Furthermore, majority of the respondents 175(58.3%) admitted that they do not downloading and installing software onto a computer in the workplace, 95(31.7%) claimed they did, while the rest 30(10.0%) were not sure.

Overall, regarding the education of information security as an influencing factor of information security awareness, findings indicate that the item "My computer has no value to hackers, they do not target me" has the highest mean compared to others (μ=2.127).

TABLE III EXTENT OF THE INFLUENCES OF EDUCATION OF INFORMATION SECURITY ON INFORMATION SECURITY AWARENESS

Education of Information security	No	Don't Know	Yes	Mean	Standard Deviation	Rank
My computer has no value to hackers, they do not target me	55(18.3%)	93(31.0%)	152(50.7%)	2.127	0.692	1
I know what to do if my computer is infected with a virus	32(10.7%)	24(8.0%)	244(81.3%)	1.973	0.432	2
I know what a phishing attack is	60(20.0%)	44(14.7%)	196(65.3%)	1.947	0.587	3
I receive training about information security in my workplace	120(40.0%)	36(12.0%)	144(48.0%)	1.640	0.687	4
I never found a virus or a trojan on my computer at work	158(52.7%)	28(9.3%)	114(38.0%)	1.567	0.659	5
I always download and install software on my computer at work	175(58.3%)	30(10.0%)	95(31.7%)	1.517	0.672	6

3. Research Question 3: What are the influences of knowledge of technology on information security awareness among non-academic staff?

TABLE IV EXTENT OF THE INFLUENCES OF KNOWLEDGE OF TECHNOLOGY ON INFORMATION SECURITY AWARENESS

Knowledge of Technology	No	Don't Know	Yes	Mean	Standard Deviation	Rank
I know what an email scam is and how to identify it	5(1.7%)	84(28.0%)	211(70.3%)	2.263	0.478	1
I know what the risk is when opening e-mails from unknown senders; especially if there is an attachment	9(3.0%)	45(15.0%)	246(82.0%)	2.120	0.407	2
I have installed, updated and enabled antivirus software on my computer	7(2.3%)	37(12.3%)	256(85.3%)	2.100	0.370	3
I know how to use antivirus software and how to scan for viruses	10(3.3%)	12(4.0%)	278(92.7%)	2.007	0.271	4

E. Knowledge of Technology

Table IV presents the results of the extent of the influences of knowledge of technology among non-academic staff on information security awareness. Results show that 211(70.3%) of the respondents knew what an email scam was, and how to identify it. In the interim, 84(28.0%) of the respondents were not sure and only 5(1.7%) said no.

Moreover, majority of the respondents 246(82.0%) knew the risk of opening unsolicited emails, 45(15.0%) were not sure, and only 9(3.0%) said no. Similarly, result shows that 256(85.3%) of the respondents knew how to handle antivirus software, 37(12.3%) were not sure, while 7(2.3%) said no. Furthermore, larger percentage of the respondents 278(92.7%) knew how to use antivirus software, 12(4.0%) were not sure, while the rest 10(3.3%) said no. However, result demonstrates that all items on knowledge of technology towards information security awareness are very important, with the item "I will make sure that when I delete a file from the computer or USB stick, that the information is recoverable" having the highest mean(μ=2.263) compared to others.

4. Research Question 4: What are the influences of employee's behaviour on information security awareness among non-academic staff?

F. Employee's Behaviour

Table V sought to identify the effect of employee's behaviour on information security awareness. Majority of the respondents 188(62.7%) asserted that if they deleted a file from the computer or a USB stick, they could recovered such information, 92(30.7%) said that they don't know, and the rest 20(6.7%) said no. Also, 267(89.0%) of the respondents agreed that they never gave their work password to anyone else, while, 24(8.0%) gave away their password, and 9(3.0%) were not sure. Similarly, 259(86.3%) of the respondents admitted that they do not share their passwords, 36(12.0%) said no, while 5(1.7%) claimed they don't know.

Likewise, 236(78.7%) of the respondents felt that their organisation's PC was safe, 48(16.0%) answered no, while 36(5.3%) were not sure. Furthermore, majority of the respondents 242(80.7%) did not use the same password for their work and personal accounts, 38(12.7%) used the same password for both, while 20(6.7%) claimed they don't know. Besides, 251(83.7%) of the respondents did not take information from the office to their various home to work on, 47(15.7%) answered yes, while less than 1% were not sure. Finally, results reveal that the item "I will make sure that when I delete a file from the computer or USB stick, that the information is recoverable" has the highest mean (μ=2.240) compared to others.

TABLE V EXTENT OF THE INFLUENCES OF EMPLOYEE'S BEHAVIOUR ON INFORMATION SECURITY AWARENESS

Behaviour	No	Don't Know	Yes	Mean	Standard Deviation	Rank
I will make sure that when I delete a file from the computer or USB stick, that the information is recoverable	20(6.7%)	92(30.7%)	188(62.7%)	2.240	0.563	1
I never give my work password to someone else	24(8.0%)	9(3.0%)	267(89.0%	1.950	0.328	2
I do not share my work password	36(12.0%)	5(1.7%)	259(86.3%)	1.897	0.356	3
I feel that my organisations' personal computer is safe	48(16.0%)	36(5.3%)	236(78.7%)	1.893	0.450	4
I use the same password on my work and personal accounts	242(80.7%)	20(6.7%)	38(12.7%)	1.260	0.572	5
I often take information from the office and use a computer at home to work on it	251(83.7%)	2(0.7%)	47(15.7%)	1.170	0.394	6

G. Percentage Distribution of Elements of Information Security Awareness among Non-Academic Staff

TABLE VI PERCENTAGE DISTRIBUTION OF INFORMATION SECURITY AWARENESS ELEMENTS

Information Security Awareness	No	Don't Know	Yes	Mean	Standard Deviation	Rank
I am aware of the information security aspects relating to my job (e.g. when to change my password or which information I work with is confidential)	10(3.3%)	50(16.7%)	240(80.0%)	2.133	0.428	1
Information security is necessary in my organisation to protect information	5(1.7%)	28(9.3%)	267(89.0%)	2.077	0.323	2
Do you think that it is ok to violate any rules if problems do not occur?	260(86.7%)	30(10.0%)	10(3.3%)	1.233	0.617	3

H. Information Security Awareness

Table VI reveals that majority of respondents are aware of information security. This was established by 240(80.0%) of the respondents answered yes about the awareness of information security aspect relating to their job, 50(16.7%) remained unsure, while less than 10(4.0%) said no. Also, results show that 267(89.0%) of the respondents answered yes about the necessity of the information security to protect information in the organisation, 28(9.3%) were not sure, while 5(1.7%) said no. In the same way, 260(86.7%) of the respondents did not agree about violating any rules if a problem does not occur, 30(10.0%) were not sure, while less than 10(3.3%) answered yes. Lastly, results ascertain that the item "I am aware of the information security aspects relating to my job" has the highest mean (μ=2.133) compared to others.

VIII. CONCLUSION

The study focused on information security awareness among non-academic staff in the University of Ibadan. Findings revealed that information security awareness is influenced by policy of information security, education of information security, knowledge of technology and non-academic staff's behaviour. Also, findings show that level of information security awareness among non-academic staff in the University of Ibadan was high. This is an indication that non-academic staffs in the University of Ibadan are aware of the possible threats and risk associated with information security. Information security awareness is considered as being crucial to the organisation, the essence of information security is to ensure continuous and smooth running of business operation without interference in an organisation. This finding is consistent with the findings of Fakeh *et al.,* (2012) and Oladipupo (2019), where they all found out that policy of information security, education of information security, knowledge of technology and non-academic staff's behaviour have influenced information security awareness. However, analysis of the data attained from the study needs to be enhanced; the study participants were basically from a single University in Nigeria. This could potentially reduce the generalisability of the findings. The sample size itself is comparatively small. This study can be expanded geographically by increasing the scope to cut across participants from several universities and different parts of the country. Potential correlations between some of the independent variables such age, gender, educational level, faculty and years of experience need to be considered in the future studies. In addition, other study should focus on other factors that are likely to influence information security awareness among non-academic staff in the University of Ibadan. Irrespective of these constraints; this study has been able to contribute to the existing literature in the field of information security.

REFERENCES

[1] E. Albrechtsen, and J. Hovden, "Improving information security awareness and behaviour through dialogue, participation and collective reflection, An intervention study", *Computers & Security*, Vol. 29, pp. 432-445, 2010.

[2] J. Boyce, and D. Jennings, "Information assurance: Managing organizational IT", Woburn, MA, Butterworth-Heinemann, 2002.

[3] M.D. Caroll, "Information security: Examining and managing the insider threat", *ACM Proceedings of the 3rd Annual Conference on Information Security Curriculum Development 2006 (InfoSecCD 06)*, pp. 156-158, Kennesaw, Georgia, 2006.

[4] C. C. Chen, R. S. Shaw, and S.C. Yang, "Mitigating information security risks by increasing user security awareness: a case study of an information security awareness system", Information *Technology, Learning, and Performance Journal*., Vol. 24, No.1, pp. 1-14, 2006.

[5] CISSP, CISM, R. P. Thomas, "Implementing an Information Security Awareness Program", *Security Management Practices,* Vol.14, No.2, pp. 37-49, 2005.

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

[7] ENISA, "*A Users' Guide: How to Raise Information Security Awareness*", *Annual Global Information.2006.* March 28, 2019, Retrieved fromwww.vistorm.com/uplds/EY_Global_Information_ Security

[8] J. Everet, "Internet Security awareness: switch to a better programme", *Employee Benefits Journal,*Vol. 23, No.3,pp. 14-18, 1998.

[9] S. K. W. Fakeh, M. N. Zulhemay, M. S. Shahibi, J. Ali, and M. K. Z. Zaini, "Information security awareness amongst academic librarians", *Journal of applied sciences research*, Vol. 8, No. 3, pp.1723-1735, 2012, ISSN 1819-544X.

[10] S. Flinn, and J. Lumsden, "User Perceptions of Privacy and Security on the Web", *National Research Council*, 2005.

[11] G. J. Gordon, "Ascertaining the relationship between security awareness and the security behaviour of individuals", Nova Southeastern: Nova Southeastern University, 2010.

[12] F. J. Haeussinger and J. J. Kranz, "Information security awareness: Its antecedents and mediating effects on security compliant behaviour", *34thInternational Conference on Information Systems.,* pp.1-16, 2013.

[13] S. Hansche, "Designing a security awareness program: Part I", *Information Systems.,* Vol. 9, No. 6, pp.14-23, 2001.

[14] S. Hinde , "Careless about privacy", UK., 2003.

[15] F. Kaur, and N. Mustafa, "Examining the effects of knowledge, attitude and behaviour on information security awareness: case on SME", *3rd International Conference on Research and Innovation in Information System-2013 (ICRIIS' 13).*, pp. 286-290, 2013.

[16] H. A. Kruger, and W. D. Kearney, "A prototype for assessing information security awareness", *Computer & Security.*, Vol. 25, No. 4, pp. 289-296, 2006.

[17] H. Kruger, L. Drevin, and T. Styen, "A vocabulary test to assess information security awareness", *Information Security & Computer Security.*, Vol. 18, No. 5, pp. 316-327, 2010.

[18] D. D. Maeyer, "Setting Up an Effective Information Security Awareness Program",*Information Security Solutions Europe/ SECURE 2007 Conference (Part 1).*, Warsaw, Poland, 25–27 September, Vieweg, pp. 49–52, 2007.

[19] A. Martins, and J. Eloff, "Information Security Culture," *Proc. of IFIP TC11 17th International Conference on Information Security (SEC2002).*, IFIP Conference Proceedings, Cairo, Egypt, 2003.

[20] J. Mathisen, "Measuring information security awareness - a survey showing the Norwegian way to do it", *Master's thesis*., Gjøvik University College, 2004. www.nislab.noiv Oslo

[21] A.R. NurulHidayah, "A Prototype to Evaluate Information Security Awareness Level for Teacher and Student in Secondary School", *Master Dissertation*, pp. 1-97, 2009.

[22] S. O. Oladipupo, "Determinants of Information Security Awareness among Employees of Capital Market Registrars in Lagos, Nigeria: An Empirical Study". *AsianJournal of Computer Science and Technology (AJCST).*, Vol. 8, No. 1, pp. 48-52, 2019.

[23] P. Puhakainen, "A Design Theory for Information Security Awareness", Doctoral Dissertation, Department of Information Processing Science, University of Oulu, Finland, 2006. http://herkules.oulu.fi/isbn9514281144/isbn9514281144.pdf.

[24] A. Segev, J. Porra andRoldan, "Internet security and the case of Bank of America", Communications of the ACM, Vol. 41, No. 10, 81-87, 1998.

[25] P.S. Shashi, "What are we managing - knowledge or information", *The journal of information and knowledge management systems*., Vol. 37, No. 2, 169-179, 2007.

[26] M. T. Siponen, "A conceptual foundation for organizational information security awareness", *Information Management & Computer Security.*, Vol. 8, No. 1, 2000.

[27] D. Straub, "Effective IS security". *Information Systems Research*, Vol. 1, No. 3, pp. 255-276, 1990.

[28] D. W. Straub and R. J. Welke, "Copingwith SystemsRisk: Security Planning Models for Management Decision Making", *MIS Quarterly.*, Vol.22, No.4, pp. 441–469.1998.

[29] T. Takemura, "A quantitative study on Japanese workers' awareness to information security using the data collected by web-based survey", *AmericanJournal of Economics and Administration*., Vol. 2, No. 1, pp. 20-26, 2010.

[30] M. Thomson, "The development of an effective information security awareness program for use in an organization". *Unpublished master's thesis*.,Port Elizabeth Technikon, Port Elizabeth, South Africa, 1998.

[31] M. E. Thomson and R.V. Solms, "Information security awareness: educating your users effectively", *Information Management & Computer Security.,* Vol. 6, No. 4, pp. 167-173, 1998.

[32] C. M. Trompeter and J. H. P. Eloff, "A framework for the implementation of socio-ethical controls in information security", *Computers & Security.*, Vol. 20, No. 5, pp. 384-391, 2001.

[33] R. Von Solms, "Information security management (1): Why information security is so important", *Information Management and Computer Security.*, Vol. 6, No. 4, pp. 174 – 177. MCB University Press, 1998.

[34] B. Von Solms and R. Von Solms, "The 10 deadly sins of information security management", *Computers & Security*, Vol. 23, No. 5, pp. 371-376, 2004.

[35] C. Vroom, and R. Von Solms, "Towards information security behavioural compliance", *Computers & Security*., Vol. 23, No. 3, 191–198, 2004.

[36] L. Yngstrom, and F. Björck, "The Value and Assessment of Information Security Education and Training. I*n: Proceedings of the IFIP TC11 WG11.8 First World Conference on Information Security Education (WISE1).*, Stockholm, pp. 271-292, 1999.

[37] Y. Zahri, and M. Z. Ahmad Nasir, "Future Cyber Weapons", *The Star In Tech*, pp. 1-4, 2003.