International Journal of Information Security, Privacy and Digital Forensics
Vol. 7, No. 1, June, 2023

Human Factors influencing Compliance to Cyber Security Practices by Employees of Public Universities in Southeast Nigeria

S. C. Chikwendu
Department of Sociology/Anthropology,
Nnamdi Azikiwe University, Awka, Nigeria
sc.chikwendu@unizik.edu.ng

N. P. Oli
Department of Sociology/Anthropology,
Nnamdi Azikiwe University, Awka, Nigeria
np.oli@unizik.edu.ng

Abstract- The increasing use of technology in workplaces has led to a rise in cyber threats, making it essential for employees to have adequate knowledge and skills to ensure cyber safety. The study examined the human factors that influence the cyber-security practices of employees in public universities in Southeast in Nigeria. The theory of planned behavior and diffusion of innovation theory were adopted as the theoretical framework of the study. The study adopted a mixed-methods research design which involved the use of quantitative and qualitative instruments for data collection. For the quantitative data, questionnaire was used while the In-depth Interview (IDI) guide was used to gather qualitative data. The sample size of 1068 respondents selected through the Taro Yamane statistical method of sample size determination was adopted for the study. The multistage sampling procedure involving the use of cluster and simple random sampling techniques was adopted in selecting the respondents for the study. Twelve IDI respondents were selected using the purposive sampling technique of non-probability sampling method. The quantitative data were processed using the Statistical Package for Social Sciences (SPSS) software version 20.Descriptive statistics such as simple percentages, frequency tables and graphic illustrations were used to analyze the quantitative data. The qualitative data were analyzed using content analysis. The findings indicate that while employees have some knowledge of cyber-security, they lack adequate skills and awareness to protect themselves and the university's information systems. Also, results of the study show that factors that influence cyber-security practices include organizational culture, training, motivation, and attitudes towards cyber-security. Therefore, the study recommends the development of a comprehensive cyber-security policy that incorporates employee training and awareness programs, regular system updates and maintenance, and strict enforcement of cyber-security policies. It also highlights the need for a positive organizational culture that prioritizes cyber-security and fosters a sense of responsibility among employees towards protecting the university's information systems.

Keywords: cyber-security, cyber-security practices, cyber threats, cyber security compliance, human factors

1 INTRODUCTION

Organizational or institutional compliance to cyber security practices is imperative, as non-compliance will come with unpalatable implications. In a broad sense, cyber security is seen by [1] as the collective application of strategies, security measures, plans, threats administration tactics, engagements, training, paramount practices, assurance and expertise that can be used to guide the information system, organization and related assets. It is also seen by [2] as a combination of efforts targeted at reducing cyber-attacks. Cyber security represents an umbrella term for proactive and reactive measures focused on confidentiality, integrity and availability of information, contrary to potential vulnerabilities [3]. With the enormity of data and information at the disposal of public organizations/institutions, they are predisposed to attacks from cyber attackers who will be interested in having access

to public data/information for malicious purposes especially if there are weak cyber security practices by employees in such organizations/institutions. The integrity of public data is at the core of cyber security practices by public organizations and institutions. The above view presents cyber security as the collective responsibility of employees and employers in securing the cyber space within which they operate. This is important because any breach in data could be costly.

With increasing number of cyber-attacks, organizations and institutions can face serious losses and need to consider investing in cyber security practices. This explains why some organizations are beginning to adopt a range of technical and procedural approaches to secure information (e.g. encryption and security awareness campaigns, respectively). For [4], a number of cyber security practices are adopted by organizations. There is the access control and password security option. This is explained by [4] to mean the focus on securing password and access controls to avoid unauthorized access and manipulation. They also identified data authentication option as an important cyber security practice. This option involves ensuring the reliability of data sources before they are downloaded. Malware scanners are also employed by organizations as a cyber security practice. This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware. Firewall is another cyber security practice which involves a software program or piece of hardware that helps screen out hackers, viruses and worms that try to reach the computer over the Internet. All messages entering or leaving the internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence, firewalls play an important role in detecting the malware. The final strategy as identified by [4] is the antivirus software option. Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. Antivirus software is a must and basic necessity for every system due to the level of security it offers on the cyber space. Public organizations/institutions in Nigeria appear not to be taking cyber security practices as seriously as they should. Some public organization/institutions in the country get too carried away by how cheap some security packages are and they subscribe to them without factoring in how strong and reliable those packages can be. This has given room for cyber attacks. For instance, a report from a Global Security Company, [5] recently revealed that more than 8 in 10 Nigerian organizations suffered public cloud security attack in the last one year. These attacks include ransomware, malware, exposed data, compromised accounts and crypto jacking.

Cyber security exists to ensure that the data and information of any institution is secured from cyber attacks. Cyber security practices are designed to be implemented by employees as they are often the ones who interact constantly with the cyberspace of the establishment they are working with. In this case, cyber security practices of universities are to be implemented by university staff particularly non-teaching members of staff of the university. This is because they have access to information/data that is of importance to both the university and its students. University employees are expected to play a critical role keeping university data and information safe as they are expected to be conversant with cyber security practices that will regularly ensure that university data at their disposal are not jeopardized or opened up to easy attacks from cyber attackers. Cyber security practices are also expected to be well stipulated and taught to staff members, with punishments and reward for non-compliance and compliance clearly stated out.

There are more cyber-attacks in Nigeria than any other country in Africa [6]. World ranking in cyber-attack indicates that Nigeria is on top of the list after United States and Britain but first in Sub-Saharan Africa [7]. Nigeria moved to the second position in 2021 according to [8]. Documented cases of cyber-attacks most prevalent in Nigeria include yahoo attack, hacking, software piracy, pornography, credit card or ATM fraud, denial of service attack, Internet Relay Chat (IRC) crime, virus dissemination, phishing, cyber plagiarism, spoofing, cyber stalking, cyber defamation, salami attack and cyber terrorism [9]. Indeed, Nigeria which boasts of a 38% internet penetration rate and 84 million internet users as at 2022, the highest in Africa, has suffered for years from cyber related crimes [8]

[7] recently revealed that more than 8 in 10 Nigerian organizations suffered public cloud security attack in the last one year. These attacks include ransomware, malware, exposed data, compromised accounts and crypto jacking. The universities are public organizations and they fall into this category, with constant exposure to malicious attacks. There seems to be no penalties for not adhering to cyber security practices in the universities. What this means is that staff members are at liberty to do whatever they like with university computer, without being concerned about whether they are endangering public data in the custody of the university. Technological factors are not the only key to effective information security controls; there is also a need to understand the impact of human and organizational factors on security controls in the work place [10]. A better understanding of how different factors such as organizational and environmental factors influence the implementation and effectiveness of cyber security policies and compliance is essential, as this may elucidate how different factors could lead to potential sources of security breaches and vulnerabilities within organizations [11].The relevance of this study is therefore anchored on filling the gap in knowledge on data about cyber security practices of

public universities and their employees and how this affects or influences cyber-attacks in the universities. There is no data on this as much as the researcher knows and there is need to fill this gap with this research. In view of the aforementioned problems, this study will therefore examine compliance to cyber security practices and how they affect cyber-attacks in public universities in Southeast Nigeria. The following objectives will guide the study; to examine the state of cyber-security compliance by employees of public universities in Southeast, Nigeria, to identify the human factors influencing cyber security compliance by employees of public universities in Southeast, Nigeria, to suggest measures to improve compliance to cyber security compliance by employees of public universities in Southeast, Nigeria

2 RELATED WORKS

[12] conducted a study on organizational cyber security practices in selected firms in Tamil, India. Using a survey research design and the simple random sampling technique, the researchers selected 450 respondents who were administered with questionnaires that contained relevant issues to the research. The study found that majority of the organizations (78%) adopted an employee based cyber security practice which leaves cyber security in the hands of the employees. The implication of this finding is that the employees are carried along as they are expected to execute the cyber security practices outlined by their organization. Organizations which adopt this kind of cyber security practice may have a better compliance rate because employees are likely to respond more positively to what they fully understand. The relevance of this finding to this research is that it will help bring to fore the existence of this kind of cyber security practice in public universities in Nigeria. [13] conducted a study on 'The IT way of loafing on the job: cyber-loafing, neutralizing and organizational justice'. Using a sample size of 188 respondents, a survey research design, the questionnaire and in-depth interviews as instruments for data collection, the survey which was conducted online found that majority of the respondents (89.9%) identified password protection and email source authentication as the cyber security practices employed by the organizations they work in. The present study establish whether these practices are also obtainable in public universities in Nigeria.

Perceived injustice in employment relationship will cause employees to rationalize their subsequent engagement in Internet abuses. What this finding suggests is that employees who are meted with treatments they consider unfair or unjust in their workplace will be unwilling to adhere to cyber security practices of the company. In essence, they will do whatever they believe will jeopardize the cyber security of the organization including engaging in careless cyber space practices. [14] conducted a study on encouraging information security behaviours in organizations: role of penalties, pressures and perceived effectiveness. The study selected 312 respondents from 77 organizations globally using the survey research design and simple random sampling procedure. IDIs and questionnaires were used to gather data in the study. The study found that pressures exerted by subjective norms and peer behaviors influence employee information security behaviors. Intrinsic motivation of employee perceived effectiveness of their actions was also found to play an important role in security policy compliance intentions. In analyzing the penalties, certainty of detection was found to be significant while severity of punishment was found to have a negative effect on security behavior intentions. The implication of this study is that while peer pressure influences compliance or non-compliance to cyber security practices of organizations, severity of punishment for staff who do not comply with cyber security practices of their organization does not influence or encourage compliance.

[15] conducted a study that examined the 'effects of social contextual factors on employees' compliance with organizational security policies.' The research model for the study was developed based on concepts adapted from safety climate literature that has been used to explain the safe behavior of employees in organizations. Data was collected from a sample of 140 employees from two large IT intensive organizations using a 28- item survey instrument and analyzed using structured equation modeling. The study found that Management practices, supervisory practices, and coworker's socialization were found to be positively related to employees' perception of information security climate in the organization. Perception of security climate and self-efficacy had positive impacts on compliant behavior. [16] conducted a study on Factors influencing information security compliance: an institutional perspective using the Ethiopian telecommunications cooperation as a case study. Data were collected via survey method. Questionnaire was employed as the instrument of data collection which involved 55 respondents. Multiple linear regression was used as data analysis method. The study result showed that management support, awareness and training, and accountability are leading organizational factors that shape employees behavior to comply with the existing information system security policy. This study implies that if employees are not trained, then lack of training will impact negatively on their compliance to cyber security practices of the organization or institution or even university they are employed in.

In another study conducted by [17] titled: Information Security Compliance in Organizations: An Institutional Perspective. With the use of structural equation modelling for analyzing the data collected through an online survey that involved 1,500 respondents selected across the world, the study shows that coercive pressures, normative pressures, and mimetic pressures positively influence information security compliance in organizations. It reveals that the benefits of information security compliance motivate management to strengthen their commitments at information security compliance. Furthermore, the study

finds out that social pressures do not have a significant impact on management commitments towards information security compliance. The implication of this study is that coercions on employees influences their compliance to cyber security practices of organizations. It means that coercion or pressure to comply with cyber security practices from management is a factor that influences cyber security compliance by employees.

In an effort to understand the problems related to information security posed by employees, [18] focused on computer crime by employees and investigated the relationship between the offender and the context using rational choice and situational crime prevention theories. The study was carried out in the UK using 350 respondents selected through the simple random sampling technique across companies that have experienced cyber-attacks in the last year. The study found that organizations should focus on the actual behaviors of offenders at various stages of their misuse in order to implement controls (safeguards) that would reduce the employees' ability to misuse the IS at each stage and, in so doing, effectively influence the decision-making processes of their employees. [19] conducted a study on 'public cyber security measures and risks of non-compliance'. The study focused on Small businesses in Canada. Using a sample size of 231 respondents administered with questionnaires and selected through simple random sampling technique and survey research design, the found that awareness creation, constant training and compliment to employees who constantly adhere to cyber security measures are the ways to improve compliance to cyber security practices by organizations.

The theory of planned behavior and diffusion of innovation theory were adopted as the theoretical framework of the study. The theory of planned behavior was developed by Ajzen in 1991. The theory postulates that a person's intention to exhibit a particular behavior can be predicted by three main factors including the attitude, the subjective norms of the individual and the personal control beliefs [20]. Firstly, the personal attitude of the individual largely consists of what the individual believes to be the outcome of performing the behavior and how worthwhile the person considers the outcome of the behavior. Thus, an employee will have a positive attitude towards complying to cyber security practices if he/she believes that the outcome of that action taken will be good and result to safety of university data [20]. A personal belief that compliance to cyber security measures is good for the employee and the university is more likely to motivate an employee to fully comply to stipulated cyber security measures than believing otherwise. This means that if a person does not believe that his or her compliance to cyber security measures will forestall cyber attacks on the university cyber space, the person will likely not adhere to stipulated cyber security practices.

On the other hand, subjective norms that influence a person's intent to perform a behavior consist of the individual's thoughts about other people's views concerning the behavior and how motivated the person is to act in line with social influencers [20]. The people around a university employee who may influence his/her thoughts and actions include friends, colleagues and family members. These group of persons are able to influence the employee significantly. The actions of these people and what they say to the employee are likely to shape the employee's decision to comply or not comply with stipulated cyber security measures. If these influences do not prioritize cyber security, the employee may not find the need to; prioritize cyber security either. However, if these influences prioritize and emphasize cyber security, the employee will most likely take a cue from them and prioritize cyber security in his or her own workplace.

Thirdly, personal control beliefs which are made up of the individual's self-efficacy beliefs refer to how confident one is that he/she is capable of performing a behavior. Self efficacy beliefs refer to how confident one is that he/she is capable of performing an action in the face of barriers. Also, external factors such as level of exposure, owning a computer at home and level of education may prevent one from acting on his or her personal beliefs or conforming to societal norms. For instance, an employee who may not believe that his/her work computer can be attacked may still adhere to cyber security practices simply because he\/she just wants to conform to established cyber security measures in the workplace. Overall, adherence to cyber security practices can significantly be influenced by factors that are external to the employee.

The diffusion of innovation theory explains how the adoption of new ideas and practices, such as complying with cyber security practices by employees, is influenced by several key factors. These factors include the perceived relative advantage of the practice, its compatibility with existing values and behaviors, the complexity of the practice, the ability to trial it, and its observability. Human factors such as the value placed on personal privacy and security, perception of complexity, and the opportunity to trial the practice all play a significant role in determining whether employees will comply with cyber security practices. By taking into account these factors, organizations can design effective cyber security policies that encourage compliance among employees.

3 METHODOLOGY

The study was conducted in 6 public universities in South East Nigeria. These universities were selected from three out of the 5 states in the region. The universities include Imo State University, Federal University of Technology Owerri, Chukwuemeka Odumegwu Ojukwu University, Nnamdi Azikiwe University, Enugu state university of Science and Technology and University of Nigeria, Nsukka. Public universities were selected because they were identified in the literature as being more exposed to cyber attacks due to human factors.

The mixed methods research design was adopted for this

study. The research deign involves incorporating quantitative and qualitative approaches in data collation, analysis and interpretation. The population of the study is 27, 111. From this population, a sample size of 1068 was selected as the sample size of the study. This sample size is considered representative of the entire population and gives the researcher the ability to generalize from the study. From each of the universities, 59 respondents were selected. Four IDI participants were purposively chosen for the study (two from each university, one male and one female). Data was collected using quantitative and qualitative tools. While the questionnaire was used to collect quantitative data, the In-Depth Interview (IDI) Guide was used to obtain qualitative data. The questionnaire was developed by the researcher in line with the study objectives. This enabled the researcher to collect primary data on the topic of study. The questionnaire was divided into sections. The first section contained questions on the socio-demographic data of the respondents like sex, age, marital status, highest educational qualification, etc. Other sections consisted of items designed to address the substantive issues of the research which were derived from the research questions, objectives of the study and study hypotheses. The questionnaire contained both close and open ended questions. The rationale behind open ended and close ended questions was to give the respondents room to express themselves especially on issues that may not be captured in the questionnaire. The questionnaire was structured in simple and concise English to avoid ambiguity so as to enable easy understanding of the items contained therein.

The In-Depth Interview (IDI) guide was employed to collect qualitative data. The importance of this instrument in a study of this nature is that it helped provide more detailed explanations on issues as every question asked was followed up by probes to elicit more detailed responses. Also, the IDI guide provided responses that corroborated or disagreed with data that was collected from the questionnaire. The questions for the IDI were designed in line with research questions and objectives of the study. The IDI was designed in simple English. This enabled proper understanding by the interviewees.

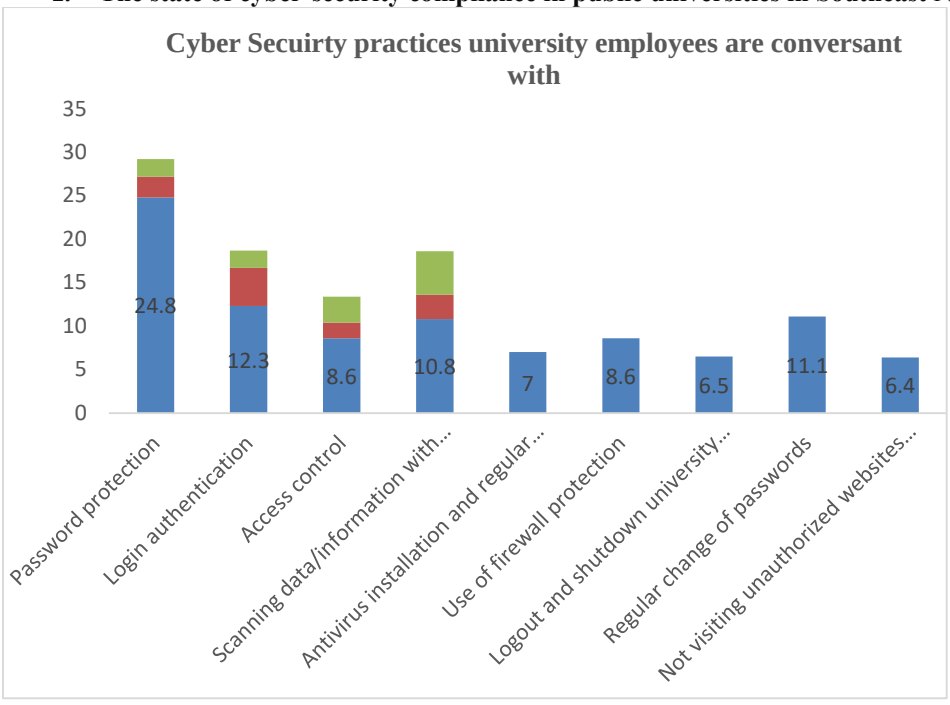
The questionnaires was keyed into and processed with the Statistical Package for Social Sciences (SPSS VERSION 20) software. This involved checking the questionnaires manually to ensure they were all properly filled. This step is necessary to clean the questionnaires and ensure that only correctly filled and retuned questionnaires are included in the data analysis. This was followed up with the use of frequencies, simple percentages and graphic illustrations such as pie charts and bar chats for the presentation, interpretation and analysis of data.

4 RESULTS AND DISCUSION

Table 1: Personal Data of the Respondents

Variable	**Frequency**	**Percentage**
Gender		
Male	370	37.6
Female	615	62.4
Total	985	100
Age		
18-27	115	11.7
28-37	226	22.9
38-47	302	30.7
48-57	252	25.6
58 and above	90	9.1
Total	985	100
Marital status		
Single	103	10.5
Married	809	82.1
Divorced	9	.9
Widowed	50	5.1
Separated	14	1.4
Total	985	100
Educational Qualification		
FSLC	113	11.5
WAEC	159	16.1
HND/BSc	435	44.2
OND/NCE	215	21.8
MSc/PhD	63	6.4
Total	985	100
Department of Respondents		
Registry	358	36.3
Bursary	351	35.6
ICT/MICTU	276	28.0
Total	985	100
Staff category		
Senior	526	53.4
Junior staff	459	46.6
Total	985	100
Religious affiliation		
Christianity	800	81.2
Islam	79	8.0
African Traditional Religion (ATR)	75	7.6
Atheist	31	3.1
Total	985	100

1. The state of cyber-security compliance in public universities in Southeast Nigeria



Field survey, 2023

Figure1: Cyber security practices which university employees are conversant with

Figure 1 shows the cyber security practices in the universities that were included in this study and which of them the respondents are most conversant with. It can be observed from figure 1 above that majority of the respondents (24.8%) identified password protection as the cyber security practice they are most conversant with. A closer look at figure 6 shows that 12.3% of the respondents identified login authentication as the cyber security practice they are conversant with, 11.1% identified regular change of passwords, 10.8% identified scanning data/information with malware scanners before they are downloaded, 8.6% identified access control and use of firewall protection, 7% identified antivirus installation and regular update, 6.5% identified logout and shut down university computer whenever it is not in use instead of staying online and hibernating the computer) while 6.4% identified not visiting unauthorized website with university computers/networks as the cyber security practice they are conversant with.

Data from the interviews conducted corroborates the above findings. The views of the interviewees are reported below.

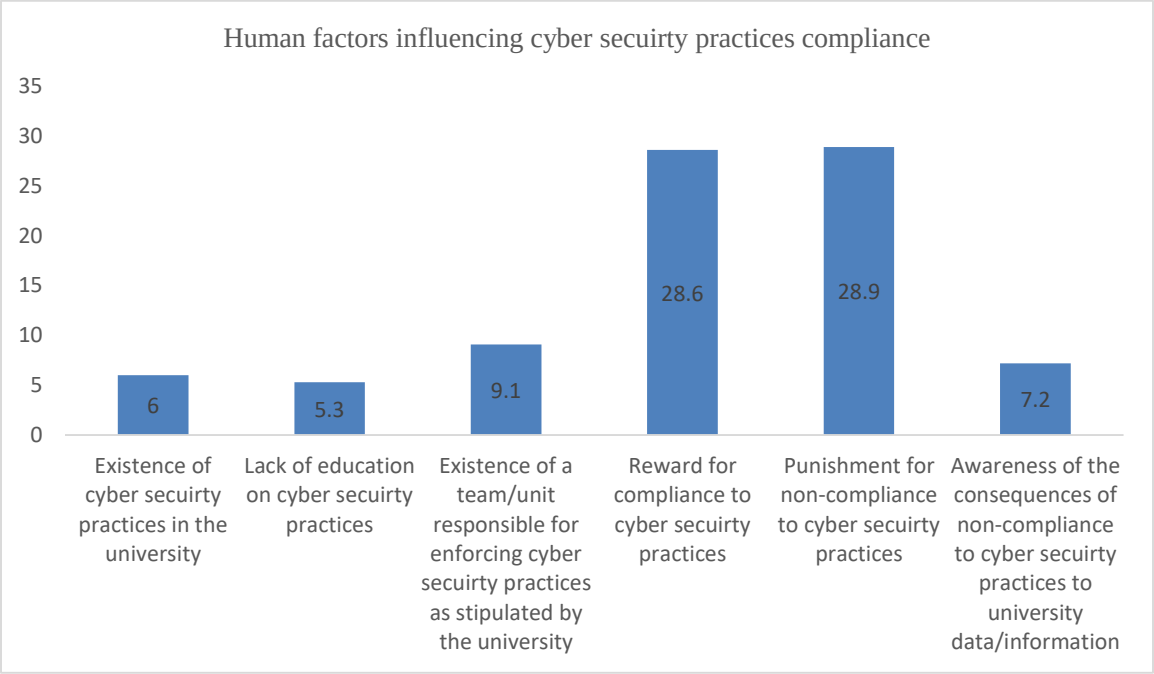
One of the interviewees had this to say:

> Personally, I am conversant with so many cyber security practices. But I think the one we emphasize more within the university environment especially among staff that handle university computers is password protection. Anybody that has access to your password can cause a lot of damage to data at your disposal. They can literally take over your computer and start operating as if you were the one and this portends a lot of danger for the university whenever it happens. Important data and information meant for such employee can be intercepted by the cyber attackers, putting university information/data at high risk. So we have password protection at the forefront of our cyber security practices in this university (Male, 32 years, married, ICT/MICTU Staff, FUTO)

Another interviewee with a similar opinion agreed that:

> Ranging from password protection to regular change of passwords, I know that there are practices that must be adhered to in order to keep the university data safe in the cyber space. There is also the practice of regular antivirus update although this is not so frequent because it requires subscription which is not always done as at when due. But password protection is emphasized as a matter of necessity to those who handle very sensitive information in the school. People can forget to adhere to these things sometimes because they are humans but that does not mean it is not usually insisted upon by those in charge. I protect my password without being told because if anything happens to my password, the university will be negatively affected (Female, 39 years, married, bursary staff, IMSU).

1. **The human factors influencing cyber security compliance by employees of public universities in Southeast, Nigeria**



Field survey, 2023

Fig 2: Human factors influencing compliance to cyber security practices by staff of Universities in Southeast

Figure 2 shows the human l factors influencing compliance to cyber security practices by staff of Universities in Southeast. From the figure, it could be observed that majority of the respondents identified punishment for non-compliance to cyber security practices as the internal factor influencing compliance to cyber security practices by staff of Universities in Southeast. Other internal factor influencing compliance to cyber security practices by staff of universities in southeast include: reward for compliance (28.6%), existence of a team/unit responsible for enforcing cyber security practices as stipulated by the university, awareness of the consequences of non-compliance to cyber security practices to university data/information (7.2%), existence of cyber security practices in the university (6.0%) and lack of education on cyber security practices (5.3).

Findings from the qualitative data also lends credence to data in figure 2. The interviewees agreed that there are internal factors influencing compliance to cyber security practices in public universities in Southeast.

One of the interviewees submitted that:

> Yes there are internal factors that could influence the compliance to cyber security practices. One of such factors is the existence of consequences for non-compliance. Human beings will mostly adhere to rules that have consequences for non-adherence. So if there are punishments for non-compliance, I believe it can improve the compliance to cyber security practices. On the other hand as well rewards can motivate the employees to comply. If there are specific rewards for compliance, there will definitely be this competition among employees to win such rewards. So yes incentives are internal factors that could trigger compliance (Male, 38 years , married, ICT/MICTU staff).

Also, another interviewee believes that:

> I would single out punishment for non-compliance as a key internal factor for compliance. This has worked for me. I have a small team that is focused on a certain project. Everyone knows what awaits them when they don't show up for their roles. Let there be clearly defined implications for not complying with certain rules. This will make everyone key into whatever rules are in the university. Cyber security is so important that there has to be consequences for not taking it serious (Female, 35 years , married, ICT/MICTU Staff).

In the same vein, another interviewee stated that:

> Anyone that fails to comply with our cyber security practices here is shut out from his/her computer for hours. This renders the person idle and frustrated with their actions. It helps keep the staff in check and also in compliance with stipulated rules and regulations for proper conduct over the cyber space this sort of punishment is encouraged. Yes there is also some sort of reward for consistent compliance (Male, 28 years , single, ICT/MICTU Staff).

Another IDI respondent stated:

> Yes the belief in the existence of cyber threats creates the consciousness to adhere to cyber security practices. This is a very important factor in my opinion. If you believe that mosquitoes cause malaria for instance, you will either fumigate your house or sleep under treated nets. So if people believe that these threats exist, they will do the right things. Efforts have been made to educate people to constantly see that there are threats with the internet generally (Female, 35 years, married, ICT/MICTU Staff).

2. Measures to improve compliance to cyber security compliance by employees of public universities in Southeast, Nigeria

Table 3: Respondents' views on whether they believe that the cyber security practices of university employees can be improved

Responses	***Frequency***	***Percentage***
Yes it can be improved	914	92.8
No I don't think so	20	2.0
I am not quite sure how this will be possible	51	5.2
Total	985	100

Field survey, 2023

Table 3 shows that majority of the respondents (92.8%) believe that the cyber security practices of university employees can be improved. On the other hand, 20 (2.0%) indicated that they don't agree while 51 (5.2%) indicated that they are not quite sure how this is possible.

Table 4: Respondents' views on the measures that can be adopted to improve cyber security practices among university employees in order to mitigate the incidence of cyber-attacks on university data/information

Responses	***Frequency***	***Percentage***
Universities that do not have cyber security practices come up with one for their employees	213	21.6
Employees should be educated on the cyber security practices of the university instead of allowing them to figure out things themselves	123	12.5
There should be a unit in charge of monitoring the cyber security practices by employees	135	13.7
The university should prioritize updating the securities in their computers in order to protect vital data	133	13.5
There should be clearly spelt out punishments for employees who fail to comply with stipulated university cyber security practices	180	18.3
The government should come up with compulsory laws mandating the universities to develop and implement cyber security practices in order to protect public data in their custody	130	13.7
Not applicable	71	7.2
Total	985	100

Field survey, 2023

Table 2 shows the measures that could be put in place to improve cyber security practices among university employees in order to mitigate the incidence of cyber-attacks on university data/information. Specifically, table 2 shows that majority of the respondents (21.6%) are of the opinion that universities that do not have cyber security practices come up with one for their employees as the measure to improve cyber security practices compliance. Other measures identified in table 2 include: Employees should be educated on the cyber security practices of the university instead of allowing them to figure out things themselves (12.5%), there should be a unit in charge of monitoring the cyber security practices by employees (13.7%), the university should prioritize updating the securities in their computers in order to protect vital data (13.5%), there should be clearly spelt out punishments for employees who fail to comply with stipulated university cyber security practices (18.3%) and the government should come up with compulsory laws mandating the universities to develop and implement cyber security practices in order to protect public data in their custody (13.7%). The question did not apply to 7.2% of the respondents. Data from the qualitative data corroborates this finding.

An interviewee stated:

> I will speak to this from what I think should be done and also from experience. First of all, I want the university to come up with very clear cyber security protocols. These protocols must contain clear, specific and measurable steps that all staff members who handle university computers must follow. Time should be taken to teach them what the right conduct is over the internet when they are working with university computers. Also, those that are not working over the internet must be guided on how to safeguard the computers they work with. I believe one of the things that the employees should be made to learn and adhere is safety. When this is done, the right action will be taken by the employees, making university information safer (Male, 33 years , married, ICT/MICTU Staff).

Another interviewee stated:

> Yes there are measures that could be employed to ensure adequate compliance to cyber security practices. Firstly, the universities without cyber security practices must as a matter of urgency come up with one. Secondly, there should be effort to teach university staff the importance of cyber security compliance. Thirdly, there should be consequences or punishment for those who do not

> adhere to laid down rule or regulations concerning cyber security by the university. People should be made to understand that not adhering to cyber security practices is a clear case of university information/data sabotage. I also believe that those in authority in the university should realize the importance of cyber security. It is only when they do that they will make efforts to ensure adherence (Male, 28 years , single, ICT/MICTU Staff).

In the same token, one of the interviewee believes that:

> Measures like university authority paying attention to cyber security in their university can be employed. Then I expect the government to also help with regulations that cut across all the universities. With a clear regulation from the state or federal government, I believe the universities will begin to pay greater attention to cyber security. The management will be mandate by such government regulations to put cyber security in the first line charge and no longer something they do when they find it convenient or when there is a problem threating the university (Female, 40, married, bursary staff).

Also, one of the interviewees stated:

> In clear terms, there are no cyber security practices here. I believe this can be changed. The people in charge can liaise with the ICT staff and come up with rules for us to guide cyber space interactions. Anybody that fails to adhere to the rules should be queried or sanctioned by the university management. This will save us the stress of bothering about frequent cyber-attacks and holding hostage of university website which we have witnessed in the past (Male, 51 years, married, registry staff).

The study found that the compliance rate to cyber security practices in public universities in the southeast is high. Majority of the respondents indicated that they comply with cyber security practices often. However, further findings show that the respondents report cyber security breaches sometimes instead of every time that it happens. The rationale for this could be because they do not want to be held responsible or punished for such breaches. One of the theoretical frameworks for this study explains this clearly. The rationale choice theory talks about people taking actions based on perceived benefits/rewards. If reporting cyber security breach would result to punishments or queries, respondents will naturally not be willing to report. However, if there are no punishments or consequences associated with doing so, respondents will show significant level of willingness to report breaches or non-compliance to cyber security practices.

Further findings show human factors influencing compliance to cyber security practices by staff of public universities in Southeast Nigeria. Majority of the respondents agreed that there are internal and external factors influencing compliance to cyber security practices in the study area. On the factors that can influence compliance to cyber security practices by staff of public universities in southeast, majority of the respondents identified punishment for non-compliance to cyber security practices. Other human factors that can influence compliance to cyber security practices by staff of public universities in southeast includes existence of cyber security practices in the university, lack of education on cyber security practices, existence of a team/unit responsible for enforcing cyber security practices as stipulated by the university, reward for compliance to cyber security practices and awareness of the consequences of non-compliance to cyber security practices to university data/information. Other factors responsible for compliance to cyber security practices, majority of the respondents identified belief in the existence of cyber security threats as the external factor that enhances compliance to cyber security practices. In this sense, people believe that cyber security threats are real. It is this belief that informs their decision to comply with cyber security practices stipulated by their universities. Lim (2022) conducted a study on 'The IT way of loafing on the job: cyberloafing, neutralizing and organizational justice'. The study identified perceived injustice or punishments as reinforcing non-compliance to cyber security practices stipulated by an organization. When employees feel that they are not being treated fairly or that they are being punished for some actions they took or they failed to take at work, they tend to strengthen their desire for non-compliance to cyber security practices. This is further explained by the rationale choice theory. People are usually rationale in their decision to comply with laid down cyber security practices. Cyber security practices that encourage punishment for non-compliance can resort to increased non-compliance while those that emphasize reward for compliance can result to increased compliance. So rewards play very important roles in the choices of university employees to comply with cyber security practices.

5 CONCLUSION

Compliance to cyber security practices is important in order to prevent cyber-attacks that could arise from non-compliance. This is the findings from this study. It has been established that there are several human factors influencing compliance to cyber security practices. These factors were found to be very important factors that measures should be put in place to address in order to ensure that university data is protected.

In the same vein, the following recommendations are put forward:

1. Universities that do not have cyber security practices should come up with one for their employees. The universities should design and circulate clearly articulated cyber security practices that will guide staff conduct over they cyber space whenever they are working with university computers, gadgets or platforms.

2. Employees should be educated on the cyber security practices of the university instead of allowing them to figure out things themselves. University employees who are not conversant with cyber security practices and its importance should be trained by the university's' ICT/MICTU unit on the cyber security practices of the university so they can be equipped with the right knowledge and information required to function and carry out their official duties without excessive vulnerability to cyber-attacks.
3. There should be clearly spelt out punishments for employees who fail to comply with university stipulated cyber security practices. University employees can sometimes act as the weak link that makes cyber-attacks possible. There should be clearly spelt out punishments like locking the employee out of his/her work computer for some hours or days so they can realize the enormity of the infarctions they committed.

References

A Growing Challenge for Security Agencies. African Journal of Criminology and Justice Studies, 11(1), 57-75.

A. AlKalbani, H. Deng, B. Kam and X. Zhang (2017). Information security compliance in organizations: An institutional perspective. *Data and Information Management*, *1*(2), 104-114.)

A. Meed (2020). Cybersecurity: Practical tips for individuals and organizations. Routledge.

C. Madu (2020). Nigeria leads in Africa's cybercrimes. The Guardian. https://guardian.ng/business-services/nigeria-leads-in-africas-cybercrimes/

E. Effiong (2021). Nigeria becomes world's second highest producer of cybercrime behind US. Techpoint Africa. https://techpoint.africa/2021/06/04/nigeria-second-highest-cybercrime-producer/

H. Chiroma and H. Ibrahim (2011). Cybercrime in Nigeria: Causes, Effects, and Remedies. European Journal of Scientific Research, 49(1), 101-111.

International Telecommunication Union. (2004). ITU internet report 2004: The internet and ICTs:

Internet for social, economic development. International Telecommunication Union.

M. Sophos (2020). Sophos Cloud Optix Threat Report: Public Cloud Security Incidents in 2020. https://secure2.sophos.com/en-us/content/white-papers/sophos-cloud-optix-threat-report-public-cloud-security-incidents-in-2020-wp.pdf

O. O. Olusola, F. A. Alaba, O. O. Ogunleye and M. A. Adebiyi (2018). Cybercrimes in Nigeria:

P.V Reddy and R. S. Reddy (2014). Cyber security: Issues, challenges and solutions. International Journal of Advanced Research in Computer Science and Software Engineering, 4(4), 281-287.

R. Solms and S. H. Solms (2017). Fundamentals of cyber resilience: An organizational perspective. CRC Press.

T. Herath & H. R. Rao (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125.