Practicum Psychologia 13, 19-39
©The Author(s) May 2023
http://journals.aphriapub.com/index.php.pp
**ISSN**: 2006-6640

# Cyber Security Practices in Public Universities in South-East Nigeria

**Chilaka Stephen Chikwendu[1] and Nneka Perpetua Oli[2]**
Department of Sociology/Anthropology, Nnamdi Azikiwe University, Awka

[1]Corresponding Author: Sc.chikwendu@unizik.edu.ng

## Abstract

The study examined cyber security practices in public universities in south-east Nigeria. Different public universities are employing various forms cyber security practices in order to protect their information from being compromised by cyber-attacks. This study seeks to find out the cyber security practices these public universities put in place to protect their cyber space. A mixed-methods research design was adopted in the study. The sample size of the study was 985. Quantitative and qualitative instruments were used to collect data in the study. A questionnaire was developed to collect quantitative data, while an IDI Guide was used to collect the qualitative data. The data were processed with Statistical Package for Social Sciences (SPSS) 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. Findings from the study show that password protection is the most common cyber security practice employed by public universities in southeast Nigeria to protect data/information at their disposal from cyber-attacks. The study recommends that 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 the cyber space whenever they are working with university computers, gadgets or platforms.

Keywords: cyber security, public universities, cyber-attacks, password protection, south-east

## Introduction

Cybersecurity exists to ensure that the data and information of any institution are secured from cyberattacks. Cybersecurity 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, the cyber security practices of universities are to be implemented by university staff, particularly non-teaching members of staff. This is because they have access to information and data that are important to both the university and its students. University employees are expected to play a critical role in 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 is 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 rewards for non-compliance and compliance clearly stated.

Cybersecurity practices constitute actions taken by organizations or institutions to ensure cyberspace safety from known and unknown threats. World-wide, cyber security breaches have been experienced and are still being experienced by public and private organizations and institutions. For instance, in April 2011, one of the biggest data breaches in corporate history took place. Sony PlayStation and Online Entertainment were hacked, and 102 million customers' credentials were stolen (Shackelford, 2012). In total, this cost Sony between one and two billion dollars directly. Sony is not the only company that has been hit by cyberattacks. According to recent numbers, almost 80 percent of US companies suffered financial losses due to data breaches and computer breaches emanating from the above-mentioned attack (Shackelford, 2012). Some estimate that one in five to one in ten computers are infected with some sort of malware, often without the owner's knowledge (Bauer & Van Eeten, 2009). More recent attacks have been witnessed elsewhere. In the UK, cyber security breaches occur on a weekly basis. The cost of each of these breaches that occur is put at $2.7 million by Ponemon (2019). Cases involving ransomware viruses that demand payments from the users of computers they infect have risen so sharply in Japan that the National Police Agency (NPA) has begun referring to the threat they pose as extremely serious. According to major cyber security software company Trend Micro Inc. (2020), 93 ransomware infections were reported by corporations in Japan, an 80% increase on the previous year. The NPA also received 23 consultations from affected firms and others. In ransomware attacks, cybercriminals encrypt without warning the internal data of corporations and other entities. They then demand virtual currency or another payment to restore the data. In Nigeria, cases of cyber security breaches have been on the rise, especially within public organizations and institutions without established cyber security practices.

As part of a wider analysis of cyber security practices within organizations, Von Solms (2000) separated the evolution of cyber security countermeasures within organizations into four generational "waves". The first generation of cyber security countermeasures existed up until the early 1980s and can be characterized as the "Technical Wave". In this generation, cyber security countermeasures focused on mainframes and data centers, where solutions focused on enhancing the cyber security of the operating system through access control lists, user IDs, and the use of passwords. In addition, physical security barriers were also the norm. The second generation of countermeasures (the "Management Wave") lasted from the early 1980s to the mid-1990s and emerged with management within organizations realizing that security was no longer just a technical issue. Hence, organizations needed to develop cyber security policies and procedures and integrate managers and executives in the security decision-making process. The third generation of countermeasures (the "institutional wave") started in the mid-1990s and continued into the early 2000s. This wave is characterized by the demand for organizations to implement cybersecurity standards and best practices. As a result, many organizations are expected to implement standards and best practices such as the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001 standard. The fourth-generation wave (Von Solms 2006) (the "Information Security Governance Wave") developed at the turn of the millennium and emerged as a result of new legal and regulatory requirements dictating that organizations implement cyber security policies and processes to protect information and information systems. Therefore, this wave defines that an organization’s security governance is included and part of its overall corporate governance posture. Nigerian public organizations and institutions appear not to be doing enough as regards the Information Governance Wave, which focuses on integrating cyber security into an organization’s security protocols and priorities.

Vance, Siponen and Pahnila (2012) 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. Lim (2022) 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 purpose of this research is to identify the cyber security practices obtainable in public universities in Nigeria.

## Methodology

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 area of the study is the South-East geopolitical zone of Nigeria. The South-Eastern part of Nigeria comprises of five states namely: Abia, Anambra, Enugu, Ebonyi and Imo States. The geopolitical zone was part of the defunct Eastern region. The area is bounded in the North-West by Kogi and Benue States, in the North-East by Cross River State, in the South by Akwa Ibom and Rivers States and in the West by Delta State. the study organizations for this study include public universities in the region. Public universities were chosen as the study organization because literature has identified the educational sector as one of the top three public sectors at risk of cyber-attacks. Public universities were further selected for the study because they are public institutions with the probability of having high rate of non-compliance or non-existence of cyber security practices, a feature common with government owned establishments in Nigeria. Hence, was necessary to find out the efforts being made by the educational sector in general and universities in particular to ensure compliance to cyber security practices and ward off cyber attackers. The universities include federal and state government owned universities in the region. These public universities have important data that are of interest to cyber attackers and there appears to be little effort towards cyber security practices compliance by staff and even management of the universities. This justified the rationale behind choosing these universities. The universities that were selected for the study are: Imo State University (IMSU), Owerri, Federal University of Technology, Owerri (FUTO), Chukwuemeka Odumeggwu Ojukwu University (COOU), Nnamdi Azikiwe University (NAU), Awka, Enugu State University of Science and Technology (ESUTH) and University of Nigeria, Nsukka (UNN).

The total population of this study is 27,711. This represents the total number of non-academic staff in the 10 universities selected for the study. The target population of this study includes the non-academic staff members of Government owned universities in South-East. The population of the study was selected from this category of staff members because they are in charge of university records, information and perform administrative duties with the use of computers belonging to the universities. The total population of the study is 27,711 (Personnel records of the 10 universities included in this study, 2021). The target population includes all the non-teaching staff (males and females) of the selected universities. A breakdown of this population by institution is shown below.

**Table 1: Distribution of non-academic staff in public universities in Southeast**

| **S/N** | **Name of University** | **Population of Non-teaching Staff** |
|---|---|---|
| **1** | Imo State University, Owerri. | 1350 |
| **2** | Chukwuemeka Odumegwu Ojukwu University. | 1051 |
| **3** | NnamdiAzikiwe University, Awka | 5332 |
| **4** | Federal University of Technology, Owerri | 1450 |
| **5** | Enugu State University. | 1315 |
| **6** | University of Nigeria, Nsukka. | 7213 |
| **7** | Abia State University, Uturu | 743 |
| **8** | Federal University of Agriculture, Umudike | 5798 |

| | | |
|---|---|---|
| **9** | Ebonyi State University | 1121 |
| **10** | Alex Ekwueme University, Ndufu-alike | 2338 |
| | **Total** | **27, 711** |

*Source: Personnel Records of Universities in Southeast as at 2021.*

The sample size of this study is put at 1068. This sample size is representative of the entire population of non-academic staff members in the selected universities. The probability and non-probability sampling techniques were adopted for this study. The probability sampling technique was used to select respondents for the quantitative data. The importance of using the probability sampling technique is that it gives all elements of the population equal chance of being included in the study. It also makes it possible to generalize findings gotten from the research as the data are often reliable due to its representative nature of the entire population. The multi-stage sampling procedure which is a combination of probability sampling techniques was adopted for this study. First, the universities in the Southeast were clustered into two groups namely: federal (cluster A) and state universities (cluster B). The names of the federal universities in Cluster A include: Federal University of Technology, Owerri, Nnamdi Azikiwe University, Awka, Alex Ekwueme University, Ndufu-Alike, Ebonyi State, Federal University of Agriculture, Umudike, Abia State and University of Nigeria, Nsukka. The names of the state universities in Cluster B include: Imo State University, Owerri, Abia State University, Uturu, Chukwuemeka Odumegwu Ojukwu University, Enugu State University and Ebonyi State University. Then using the balloting method of simple random sampling technique, 3 universities were selected from each cluster. In cluster A, Federal University of Technology Owerri, Nnamdi Azikiwe University Awka and University of Nigeria, Nsukka are the federal universities that were selected from cluster A. In cluster B, using the same balloting method of simple random sampling technique, 3 universities were selected. The universities that were selected from cluster B include: Imo State University, Owerri, Chukwuemeka Odumegwu Ojukwu University and Enugu State University.

In the 6 selected universities, non-academic staff are divided into Registry, Bursary and ICT/MICTU units. Using the purposive sampling technique, these 3 departments were selected in the study in order to obtain a balanced sample from all categories of non-academic staff in the university. So from each university, respondents were selected from 3 departments. This brought the total number of departments included in the study to 18. In each department, the researcher adopted the simple random sampling technique of balloting method to select 59 respondents. The table below gives a breakdown of the universities that were studied, departments/units that were included in each university and the number of respondents that were selected from each department/unit.

Data were collected using quantitative and qualitative instruments of data collection. 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.

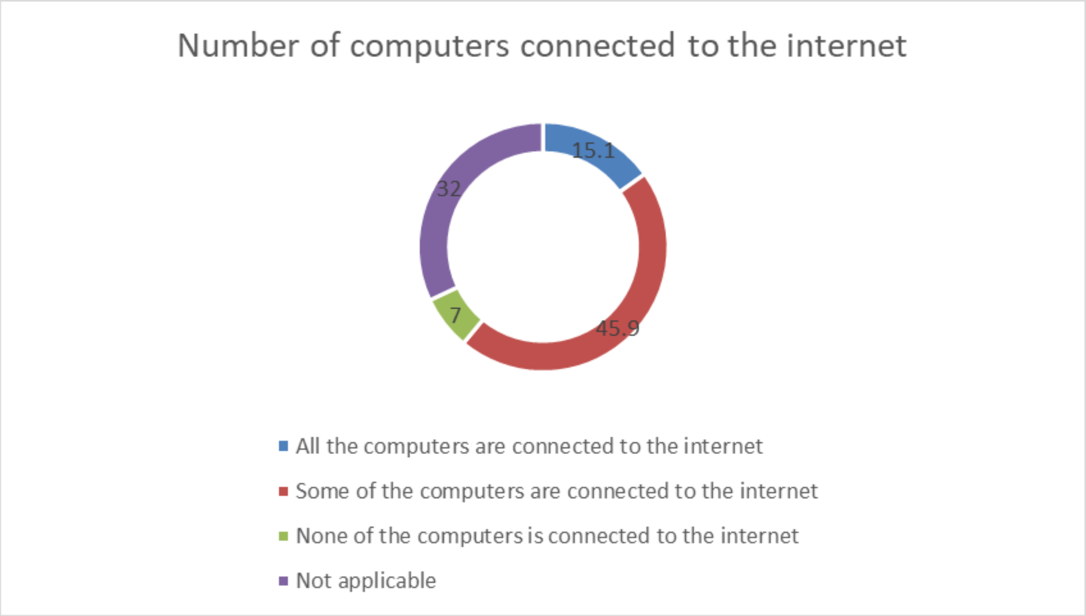
## Results

**Table 4: Respondents' views on whether their job involves access to and usage of an internet connected computer**

| *Responses* | *Frequency* | *Percentage* |
|---|---|---|
| Yes | 670 | 88.0 |
| No | 315 | 32.0 |
| Total | 985 | 100 |

**Field Survey, 2023**

Table 4 shows that majority of the respondents (88.0%) indicated that their job involves access to and usage of an internet connected computer wile 315 (32.0%) indicated that their job does not involve access to and usage of an internet connected computer. This implies that the job done by most non-academic staff members of the university involves the use of a computer which puts the data/information of the university at risk of cyber-attack.



Field Survey, 2023.

**Fig 1: Respondents' views on the number of computers connected to the internet in their offices/universities**

Figure 1 shows that majority of the respondents (45.9%) are of the opinion that some of the computers in their offices are connected to the internet. On the other hand, 15.1% indicated that all the computers in their offices are connected to the internet while just 7% of the respondents indicated that none of the computers in their office is connected to the internet. This implies that majority of the computers in the universities included in this study are connected to the internet. While some of the respondents interviewed agreed with the above finding, the views of other interviews shows a sharp contrast from this finding.

In agreeing with the data from figure 5, one of the interviewees stated:

> I would say most of the computers are connected to the internet because I was part of the team that worked on the installation of internet in most of the offices here in the administrative block of the university. From the bursary department to the registry department and its sub units, we connected every computer to the internet. So yes, most of the computers are internet enabled. I really cannot say if they are still connected because maintenance is another challenge with some of these facilities (Male, 31 years, Single, ICT/MICTU Staff at UNN).

In the same vein, another interviewee stated:

> We don't have the capacity to get all the computers connected to the internet but some of them are connected. In my office I can 60% connection has been achieved. In other offices we can talk about 40-50% connection as well. This is commendable

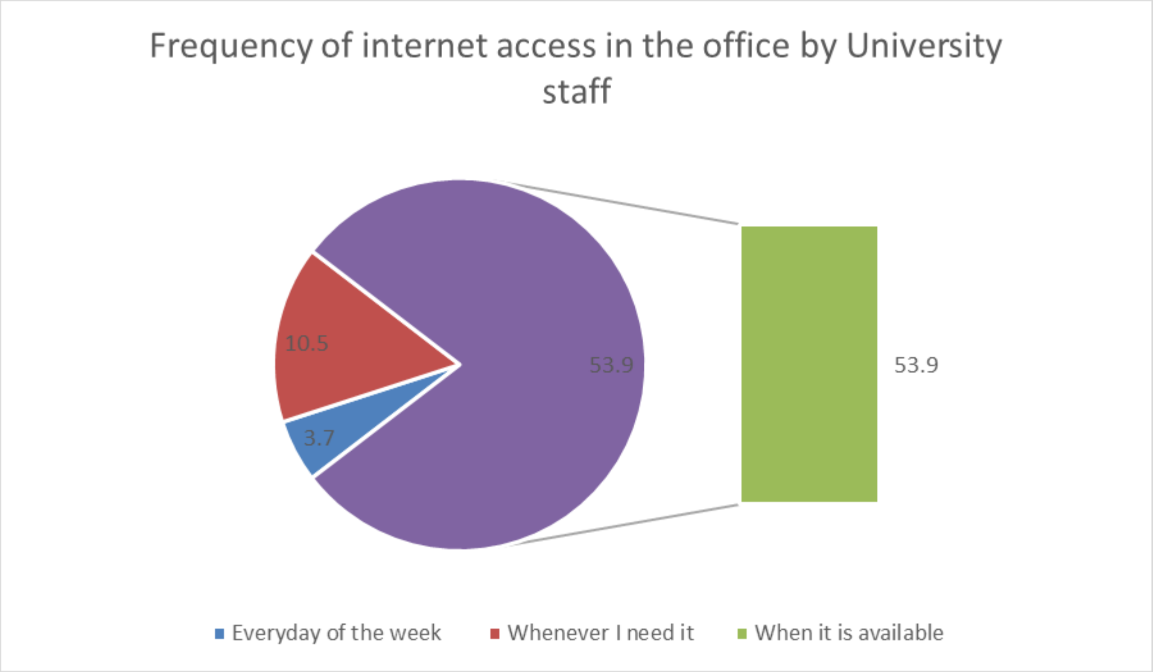
> but still more to be done. I believe the university has the capacity to connect every computer to the internet to make the work we do more effective. (Male, 43 years, married, ICT/MICTU Staff at NAU).

In disagreeing with the above data, one of the interviewees had this to say:

*'No computer in my office is connected to the internet. Most of the work we do is just type and save and then print. We don't have access to the internet at all' (Female, 45* years, *, Married, Registry Staff at COOU).*

Another interview who disagreed with the data in figure 5 stated that:

> We used to have internet connection many years ago but for over 4 years, none of these computers (points at 4 desktop computers in her office) has had internet access. We keep hearing that they will fix the problem but to no avail. I believe there is something wrong somewhere and it is also affecting our productivity because jobs that require internet access, we would have to either go outside or we do them with our phones when we have data (Male, 51 years, , married, Bursary Staff, FUTO).



Filed Survey, 2023

**Fig 2: Respondents' views on how often they access the internet in their offices**

Figure 2 shows that majority of the respondents (53.9%) indicated that they access the internet in their offices only when it is available. 10.5% indicated that they access the internet whenever they need it while 3.7% indicated that they access the internet every day of the week. The obvious implication of this finding is that internet access by university staff is hardly available every day of the week. Therefore, it is only when there is internet connection that staff members are able to go online to carry out their duties/responsibilities.

**Table 5: Respondents' views of cyber security practices as actions taken to protect data and information belonging to the university from cyber attackers**

| *Responses* | *Frequency* | *Percentage* |
|---|---|---|
| Yes, I agree | 935 | 94.9 |
| No, I don't agree | 50 | 5.1 |
| Total | 985 | 100 |

Field Survey, 2023

Table 5 shows that an overwhelming majority of the respondents (94.9%) agree that cyber security practices are actions taken to protect data and information belonging to the university in the cyber space from cyber attackers. The rest of the respondents (5.1%) did not agree with this. In essence, the respondents consider cyber security practices as important actions aimed at protecting the information belonging to the university from cyber attackers.

Questions on this research item were asked the interview participants and they agreed with majority of the respondents in table 5 above.

An interviewee stated:

> Yes that's my view too. At the core of cyber security practices is the protection of data and information. Whatever action taken to protect data and information can safely be referred to as cyber security practices. University data as I mentioned earlier is highly susceptible to cyber-attacks so there must be cyber security practices in place to ensure that those responsible for managing university data and information are aware of the right things to do (Male, 28 years, Single, ICT/MICTU Staff, ESUTH).

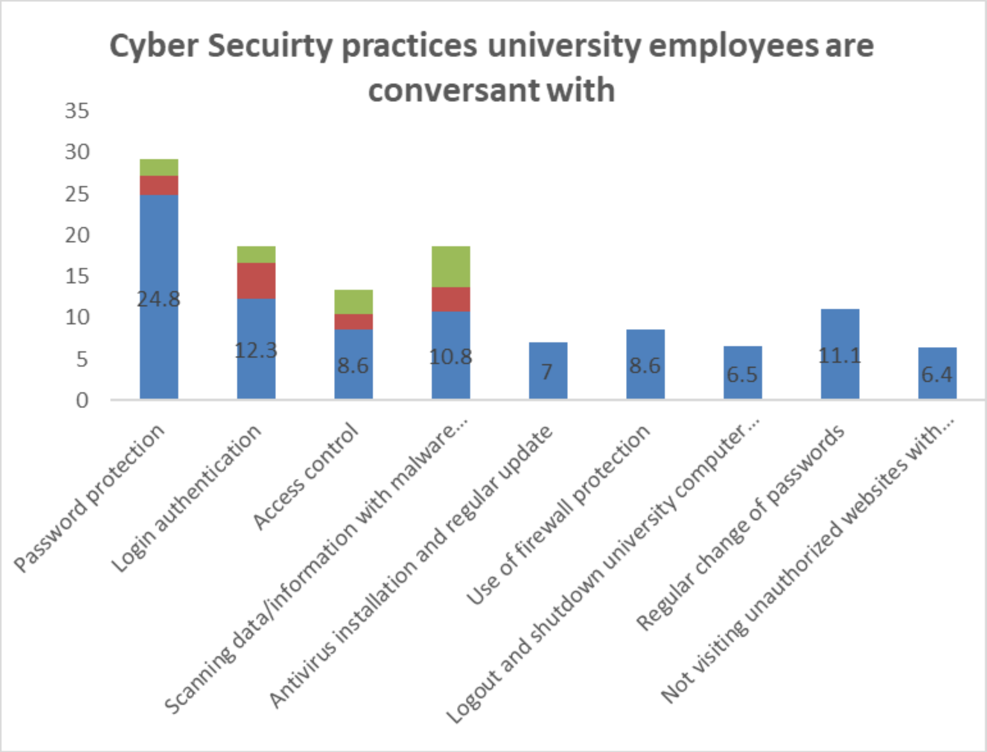
Relatedly, one interviewee stated:

> My opinion is that cyber security practices are compulsory actions that must be undertaken by university employees who utilize university computers for their work in order to keep university data and information safe and secured every day. Generally, there should be specific cyber security practice regulations for every staff

> so as to guarantee proper security of university cyber space and computers (Male, 39 years, Married, ICT/MICTU IMSU Staff).

Additionally, one of the interviewees believes that:

> Cyber security practices at the work place involve actions taken to protect data and information belonging to the university that is saved in the cyber space from cyber-attacks and cyber attackers. I agree with this because little actions taken by university employees towards reducing cyber-attacks paly very crucial roles for us. I reckon that university staff are aware of the cyber security practices that should be put in place. There might be problem with implementation but I want to believe they fully understand what cyber security practices entail (Female, 33 years, married, ICT/MICTU, COOU Staff).



**Field Survey, 2023**

**Fig 3: Respondents' views on the cyber security practices university employees are conversant with**

Figure 3 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 3 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 3 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, 31 years, Single, ICT/MICTU, UNN Staff)

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 (Male, 51 years, Married, ICT/MICTU, FUTO Staff).

One of the female ICT/MICTU staff believes that:

> Password protection is the cyber security practice most people are conversant with because they hear about it all the time. There is consciousness about passwords and the need to protect them particularly from third parties so I can affirm that everything password protection is what all university staff are conversant with. They might know little or nothing about authentication but password protection is something they are all aware of. I don't know how they are able to keep to the need for password protection but I sure know that they are aware of it (Female, 33 years, Married, ICT/MICTU, COOU Staff).

Also, another interviewee stated that:

> There are three main cyber security practice I am aware of. The first is the use of antivirus software, the second is password protection while the third is login authentication. They are very important and I believe that adequate implantation can further guarantee the protection of university data at all times because without which, cyber attackers will have a fields day doing whatever they like with university information (Male, 45 years, married, Registry Staff, ESUTH).

**Table 6: Respondents views on how they learnt the cyber security practice they are conversant with**

| *Responses* | *Frequency* | *Percentage* |
|---|---|---|
| I was taught at my workplace | 266 | 27.0 |
| I learnt them on my own | 153 | 15.5 |
| From colleagues | 425 | 43.1 |
| Social media platforms like Twitter and Facebook | 141 | 14.3 |
| Total | 985 | 100 |

**Field Survey, 2023**

Table 6 shows that majority of the respondents (43.1%) indicated that they learnt the cyber security practice they are conversant with from their colleagues. What this means is that employees who are conversant with certain cyber security practices pass such knowledge to their colleagues at work in order to ensure that they are able to also keep university data safe. More so, a significant percentage of the respondents indicated that they learnt the cyber security practice they are conversant with at their workplace. This further strengthens the data about employees learning cyber security practices from their colleagues. However, 153 (15.5%) of the respondents indicated that they leant the cyber security practice they are conversant with on their own while 141 (14.3%) indicated that they learnt from social media platforms like twitter and Facebook. Corroborating this data, the interviewees had similar views to share.

An interviewee stated:

*'I think most people learnt from the workplace. They were mostly unaware of cyber security practices until we taught them what to expect and what to do as regards safeguarding information in the cyber space' (Male,43* years,*Married, ICT/MICTU Staff NAU)*

Another interviewee stated:

> I leant from my friends and colleagues in the office. I remember one time I came to work and my password was not logging in. I was confused on what could be the problem. I didn't know my password had been compromised and I couldn't login with it anymore. It was the guys in ICT that assisted me to recover my password and also taught me how to keep it safe (Female, 43 years, Married, Bursary Staff, UNN).

One of the interviewees who learnt cyber security practice from colleagues and the social media captured his experience thus:

> When I began working here I was literally a novice on cyber security issues. I was just doing my job without factoring in cyber security. However, the day we had a cyber-attack in my office, I was wondering what could have gone wrong. I later learnt that unauthorized persons gained access into our space and we were logged out of our site. Everybody was confused and we couldn't do any work for one week before the site was recovered. Some people from our ICT unit were drafted to teach us basic cyber security practices. It was helpful but not enough. So as I got curious, I went online and began learning so many things which eventually assisted me in becoming more grounded in cyber security and safety. I now teach people in my office especially new members of staff (Male, 38 years, Married, Registry Staff, COOU).

**Table 7: Respondents' views on whether there are cyber security measures put in place by university management to guide staff operations**

| *Responses* | *Frequency* | *Percentage* |
|---|---|---|
| Yes | 436 | 44.6 |
| No | 406 | 41.2 |
| I am not sure | 140 | 14.2 |
| Total | 985 | 100 |

**Field Survey, 2023**

Table 7 shows that 44.6% of the respondents are of the opinion that there are cyber security measures put in place by the university management to guide staff operations, 41.2% indicated that there are no such measures while 14.2% indicated that they are not sure if there are existing cyber security measures to guide staff operations in the university. This shows that majority of the respondents indicated that there are existing cyber security measures to guide staff operations in the university. However, a closer look at table 7 shows that a combination of the last two options presents a higher percentage of respondents who indicated that there are no cyber security practices in their university. Responses from the interviews did not agree with data in table 9.

One of the interviewees stated that:

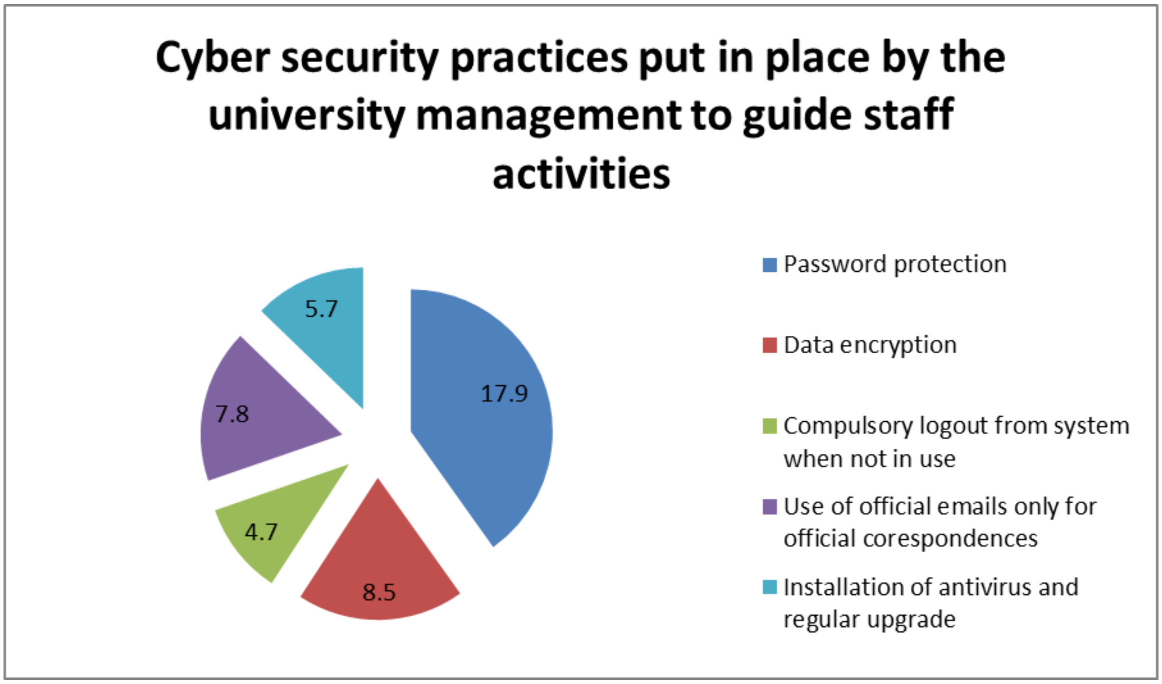
*There is no specific cyber security template in my university. People just do what they can to keep safe. But as for a unified university manual for cyber security, it is not there. We have talked about it as unit but t has not be implemented as much as I know (Male, 43* years, *Married, ICT/MICTU Staff NAU).*

Another interviewee opined that:

> You mean a unified code of conduct to guide cyber security practices? There is nothing like that. It's like a free for all affair. Ideally, there should be training for every employee and a manual to follow in conducting online or computer based operations as per cyber security practices. However, it is not obtainable here. The ICT people might just be the only ones that have something close yet it is still informal. We just police ourselves because we know what to do to keep safe online. This is hardly the same with other members of staff working in departments like registry or bursary (Male, 28 years, Single, ICT/MICTU Staff, ESUTH).

In the same token another interviewee agreed that:

> There is lack of coordination in terms cyber security practices and policy in our university. I started work with computers in my office but till date, I have not been taught anything about safety protocols that must be adhered to while working with the computer. I simply have to use my initiative all the time. This is wrong in the sense that it will give room for confusion and mistakes on the part of the employees. Most of the cyber-attacks we have experienced were things that could have been avoided if there was proper training and guidelines for conduct (Female, 37 years, Married, Registry Staff, NAU).



**Field Survey, 2023**

**Fig 4: Cyber security practices put in place by university management to guide staff activities**

Figure 4 shows the cyber security practices put in place by universities in southeast to guide staff activities on the cyber space. The most common cyber security practice in universities in the southeast as show in figure 4 is password protection (17.9%). Password protection is the most encouraged strategy by the university to ensure that data and information belonging to the university is kept safe. This is followed by data encryption (8.5%), use of offal emails only for official correspondences (7.8%), installation of antivirus and regular upgrade (5.7%) and compulsory logout from system when not in use (4.7%). The views of the interviewees corroborates the findings in figure 7.

An interviewee stated:

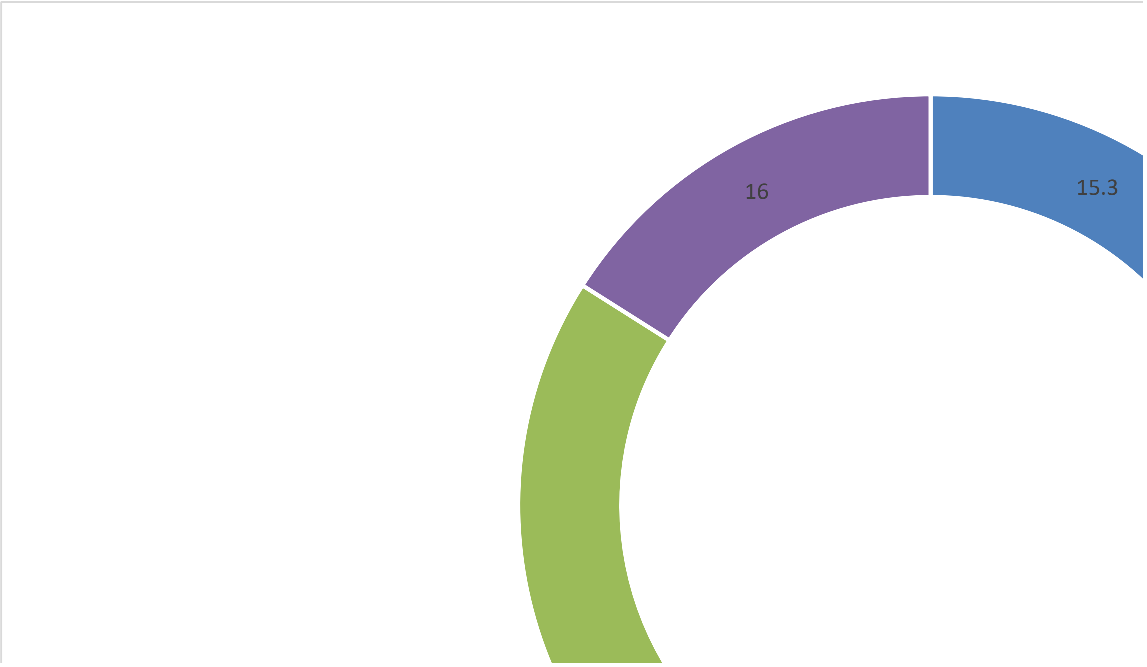
*'While there is no official cyber security measure or guideline in the university, we advise staff members to take password protection very seriously as any breach can be very fatal for public information in their custody' (Male, 31* years, *Single, ICT/MICTU Staff UNN).*

Another interviewee agreed with the above point of view when he said:

> Everybody knows the importance of password protection. We emphasize on this whenever we connect the computers for any unit to the internet. In my opinion, password protection is the major cyber security practice for us in this university. Then data encryption is also encouraged by our team leader. You should understand that the whole university does not have a clearly defined cyber security protocol for its staff so we stand in by trying to teach people what is very important (Female, 33 years, Married, ICT/MICTU Staff COOU).

Another interviewee stated that:

> *It is password protection and installation of antivirus. They take it very seriously here. Those in charge always check that the antirust is up to date. This has prevented any form of cyber-attack for the university over the years (Male, 45* years, *married, ICT/MICTU Staff).*



**Field Survey, 2023**

**Fig 5: Respondents' views on the level of attention to cyber security by universities**

Figure 5 shows that majority of the respondents (50.4%) indicated that the level of attention to cyber security in their university needs improvement. In essence, this indicates that the level of attention to cyber security in most of the universities in southeast needs improvement as there is very minimal attention to the issue. On the other hand, 18.3% of the respondents indicated that the level of cyber security in the universities in southeast is on the average, 16.0% indicated that there is no security at all while 15.3% indicated that the cyber security practices are above average.

**Table 8: Respondents' views on who sets up, maintains and troubleshoots office computers and networks in their university**

| *Responses* | *Frequency* | *Percentage* |
|---|---|---|
| An in-house ICT officer/manager | 382 | 38.8 |
| An on-call consultant | 154 | 15.6 |
| A repair service as needed | 87 | 8.8 |
| Volunteers | 177 | 18.0 |
| Staff members are on their own | 185 | 18.8 |
| Total | 985 | 100 |

Field Survey, 2023

Table 8 shows the respondents views on who sets up, maintains and troubleshoots office computers and networks in their universities. For majority of the respondents (38.8%), an in-house ICT officer/manager does this job. Other respondents indicated that an on call consultant does the job (15.6%), a repair service as needed (8.8%), volunteers (18.0%) while 18.8% indicated that staff members are on their own. The above data in table 10 was overwhelmingly supported by data from the interviews conducted.

An interviewee stated:

> We are responsible for the cyber space in this university. Setting up and maintaining the systems is primarily what we do for the whole university. Where there are challenges, we are also the ones with the responsibility of trying to fix them up. We only go outside to seek for help or assistance when the job goes beyond our capacity. But we have not had such scenario. We have been able to handle all issues regarding setting up and maintaining every computer in this university (Female, 33 years, Single, ICT/MICTU Staff FUTO).

Another interviewee had this to say:

> No going outside has not really been the option because our guys in the MICTU are very capable. They have been setting up and troubleshooting very well. We have even recently set up a bigger office o campus from where we serve the entire university community. So the ICT guys within are the ones in charge of everything

> ICT. There is no need to outsource. The Vice Chancellor has continued to equip us with the necessary tools to so well at the job (Male, 43 years, Married, ICT/MICTU Staff, NAU).

## Discussion of Findings

The study looked at the cyber security practices in existence in public universities in southeast Nigeria. The study found that password protection is the most common cyber security practice in existence in public universities in South East. Other cyber security practices identified by the study include login authentication, access control, scanning data/information with malware scanners before they are downloaded, antivirus installation and regular update, use of firewall protection, logging out and shutting down university computer whenever it is not in use instead of staying online and hibernating the computer, regular change of passwords and not visiting unauthorized websites with university computers/networks. This underscores the importance of password in safeguarding the cyber space operated by universities.

The vulnerability of university data is higher with passwords that are not protected. This explains the primacy placed on password protection by the universities in designing their cyber security practices. This finding does not align with that of Lee, Lee and Yoo (2018) who identified other cyber security practices employed by public and private organizations in tackling cyber attacks.. For universities with cyber security practices, password protection was shown to be the most important form of cyber security practice. For university employees, passwords are critical for protecting access to their computers and information contained therein. Anything that exposes passwords to unauthorized persons will put the university information and data at risk of being accessed by cyber attackers.

## Conclusion and Recommendations

Compliance to cyber security practices is important in order to prevent cyber-attacks that could arise from non-compliance. Public Universities in southeast are increasingly adopting the use of computers and the internet in their day to day operations. This explains why they are exposed to different kinds of cyber-attacks like phishing and ransomware attacks.

For universities with cyber security practices, password protection was shown to be the most important form aspect of cyber security practice. For university employees, passwords are critical for protecting access to their computers and information contained therein. This study has clearly shown that password protection is key in protecting university data and information. The study therefore recommends that;

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 the 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 that 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. The university should prioritize updating the securities in their computers in order to protect vital data. When security features in computers expire, they act as easy tools for cyber attackers. The university ICT/MICTU unit should be responsible for ensuring that security features on all university gadgets are up to date

## References

Bauer, J. M., & Van Eeten, M. J. (2009). The Economics of Spam. In S. Dietrich (Ed.), *Economics of Information Security* (pp. 259-308). Springer.

Lim, V. K. G. (2022). The IT Way of Loafing on the Job: Cyber-Loafing, Neutralizing, and Organizational Justice. *Information & Management, 59*(1), 103482.

Ponemon Institute. (2019). The Cost of Cyber Crime Study: Global. Retrieved from *https://www.ponemon.org/local/upload/file/2019%20Global%20CC%20Study%20FINAL%209-4.pdf*

Shackelford, S. J. (2012). *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*. Cambridge University Press.

Trend Micro Inc. (2020). 2020 Annual Cybersecurity Report. Retrieved from *https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/annual-cybersecurity-report-2020*

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory. *Information & Management, 49*(3-4), 190-198.

Von Solms, B. (2000). A Paradigm Shift in Information Security. *Computers & Security, 19*(5), 495-497.

Von Solms, B. (2006). Information security—The fourth wave. *Computers & Security*, 25(3), 165-168.