Research and Development in Education (RaDEn)

UMM

Research Article

Challenges of information security laws and legislations in Nigeria's institutions of higher education: Views from Yola, Adamawa state

Ngboawaji Daniel Nte[a,1,*], Vigo Augustine Teru[a,2], Arifin Ridwan [b,3]

[a] Department of Intelligence and Security Studies & Provost, College of Management and Social Sciences, Novena University, Ogume, Delta State, Nigeria

[b] Faculty of Law, Universitas Negeri Samarang, Sekaran, Gunungpati, Semarang, Central Java, Indonesia

[1] ngbodante@gmail.com; [2] profdnte@novenauniversity.edu.ng; [3] ridwan.arifin@mail.unnes.ac.id

* Corresponding author

Citation Nte N. D., Teru V. A., & Ridwan A. (2024). Challenges of information security laws and legislations in Nigeria's institutions of higher education: Views from Yola, Adamawa state. *Research and Development in Education (RaDEn), 4*(2), 1498-1519. https://doi.org/10.22219/raden.v4i2.35711

Received: 11 August 2024
Revised: 21 December 2024
Accepted: 23 December 2024
Published: 30 December 2024

Abstract: The menace of threats against information security worldwide cannot be overemphasis. The whole gamut of statecraft, national security, public safety, international trade and indeed postmodernity revolves around information security. As a country, Nigeria is part of a global system facing this monumental threat and institutions of higher education are a subset of the vulnerability circle. This work therefore seeks to evaluate the challenges of implementation of information security laws and legislations in Nigerian institutions of higher education with special focus of higher education institutions in Yola, Adamawa State. Generally, the work investigated the impact of information security threats and attacks in institutions of higher learning, the role of security laws and legislations in combating these threats, the challenges of information security threats management and indeed possible solutions to these challenges. The work utilised a qualitative research method through the application of archival and documentary research, and Case study research (multiple case study) and interviews from a selected sample. Consequently, the study was able to evaluate the state of awareness of information security in this sector, the implementation challenges of the existing information security laws and regulations and offered valuable policy recommendations to the various stakeholders on how to implement sustainable information security laws and legislations to guarantee the protection of critical data assets not just in institutions of higher education in Nigeria but the entire country and in tandem with global best practice.

Keywords: implementation laws; information security; institutions of higher education; legislation

1. Introduction

Post modernism and indeed the 4th and 5th industrial complexes are predicated on Information, Communication Technology (ICT) as its lubricant. More so, this millennium is predominantly an information one (Longo et al., 2020). The success and failure of premodern states and nations depend largely to the level of ICT penetration (Sorokoumova et al., 2021; Ukhami & Abdulsalam, 2024). It is therefore no gainsaying the fact that information, data and ideas rule the world. At the heart of this new global development reality is the challenge of information security of states, entities, institutions and the entire social system (Vázquez-Cano et al., 2022). Contemporary societies need information for planning, production, distribution and indeed the whole gamut of socio-economic and political endeavours (Kraus et al., 2022). At the heart of information management is the challenge of information security. The world is currently facing an innuendo of information security threats from hostile states, entities, organisations, institutions and non-state actors (Sigholm, 2013). From the simple hedonistic spheres of social relations to the more complex defence and industrial institutions, the threats of information insecurity have assumed a morbid and frightening dimension.

Industrial espionage, cyberattacks, election meddling, cybercrime, cyber bullying, fake news, psychological warfare and misinformation etc (Hammar, 2022; Vilmer et al.,

2015). Are the various facets information security threats that are of serious concern to nations across the world. Consequently, measures are taken by modern states in the form of laws and regulations to protect governments and citizens from the threats and attacks of cyber criminals and malevolent elements (Ukhami & Abdulsalam, 2024). Herein lies the era of information security laws and regulations. From the very advanced countries to the developing nations, concerted efforts are being made to secure the cyber and information space to guarantee public safety and national security.

In the same vein, educational institutions as part of their development trajectories have relied heavily on the fulcrum of information communication technology. Teaching and learning, knowledge development, library management, health, physical security, communication and general school administration in the education sector and especially in institutions of higher learning all over the world rely on information technology (Hasan, 2023; Okibo & Ochiche, 2014; Sorokoumova et al., 2021). In spite of the aforesaid relevance, the threat of information security looms large in higher educational institutions.

A major challenge in information security has remained the protection of the confidentiality, integrity and availability (CIA) of the available and deployed information in contemporary society and indeed different institutions including institutions of higher learning across the world including Nigeria (ISO/IEC, 2018; Jacob et al., 2020; Mitchell & Osazuwa, 2023). This obvious challenge necessitated the introduction of ISO/IEC 27001 for a sustainable information security management template known as information security management systems (ISMS). The provisions of ISMS underline the needs and designs customised to fit to all organisations and institutions (Hadzhikoleva et al., 2019). In the light of the foregoing, higher institutions in Nigeria are copiously aware of the threats that all their classified and sensitive data face, as cybercriminals are always targeting them and related institutions (Welch, 2019).

It is a well-known fact that organisations and indeed institutions of higher learning are making frantic efforts to protect the confidentiality, integrity and availability (CIA) of classified and sensitive data and critical assets in a world full of competition and sabotage (ISO/IEC, 2018). Consequently, ISO/TEC 27001 was created to provide for a sustainable data management programme known as Information Security Management System (ISMS) designed to fit into the peculiarities and needs of each organisation and institution based on type, size and goal (Hadzhikoleva et al., 2019). Within this context, it should be realised that Institutions of higher education in general house large volumes of critical data and assets and these can be quite vulnerable to cybercriminals (Welch, 2019). The study therefore looks at the prevailing information security laws and legislations in Nigeria as it relates to Information security management in educational institutions in Nigeria with special focus on institutions of higher learning in Yola metropolis in Adamawa State, North East Nigeria.

Statement of the Problem; It is common knowledge that higher institutions in Nigeria have been faced with the endemic threats and attacks such as phishing, malware, ransomware, denial of service, and network breakdown etc (Bitsight, 2016). The report further stated that Nigeria's educational sector has remained vulnerable to cyber-attacks including ransomware which has ravaged about a tenth of all the higher institutions in Nigeria. This represents thrice the incidents of attack on the health care information security system and ten times that of the financial sector in the country. In the same vein, Grajek, (2018) in Educause report showed that very minimal progress have been achieved in tackling information security breaches in the educational sector in the country. This reality has revealed an enormous challenge in information security management challenges for the third year in a row despite the measure these higher institutions of higher learning have put in place to secure their data and other critical information assets. However, it is apparent that the country is still battling with effective legal frameworks

that will provide a sustainable template for an actionable national information security policy in a world riddled with monumental information security challenges.

The Nigeria Data Protection Regulation of 2019 was established to among other things ensure the development of information technology to reposition the country among the comity of nations in the information technology race (NITDA, 2019). It also requires that organizations collecting and processing personal data of a data subject must secure such from foreseeable hazards and breaches such as theft, cyberattacks, etc. Accordingly, the regulation also mandates that those entrusted with personal data owes a duty of care to the data subject. The Institution of Higher Education have been entrusted with a huge amount of personal data of students, parents, staff members while maintaining a large amount of data on donors, funding agencies, and research output, which the law requires the Institutions Higher Education to secure (Welch, 2019).

In Nigeria, the fact remains that Institutions of Higher Education are inundated with the challenges of contemporary information technology security management in the face of recurring incidents of hacking and cyber-attacks in our higher institution by cybercriminals (Ibrahim et al., 2024). These security threats and breaches have remained a source of great concern to the Nigerian state as the custodian of the lives and property, public safety and the protection of the security of the entire citizenry. It therefore behoves the government of the country to craft implementable information security laws and legislations to aid the proper management of information security in the country (Okeshola & Adeta, 2013). It is therefore very expedient that thee education sector must be awakened to the reality of the internal and external cyber threats against the massive volume of data it currently processes and stores, and live up to expectations of the laws of the land as regards data protection.

The 2017/2018 data breach is well documented in Nigerian Universities, several data were compromised and ransomware requested huge amount of bitcoin as payment in ransom. The security breach rendered many of the institution's systems unusable for days (Garba et al., 2020). Despite this unfortunate incident, many institutions of higher learning in Nigeria, appear not to fully appreciate the enormity of the threats of data breaches and the activities of data criminals (Okeshola & Adeta, 2013). Consequently, this has undermined genuine efforts to put in place an effective information security management system to attenuate these threats. Experts have expressed deep concerns about the dire challenges of information security. According to Onohihu, (2022), realizing the need for security is one of the hardest things about security, consequently, Elhabashy et al., (2019), submitted that two types of organizations existed; those that have been hacked and those that are yet to realize they have been hacked. Okibo & Ochiche, (2014) also recorded a similar situation as above where a Kenyan university information system was hacked leading to unauthorized modification of academic grades, financial records of students thereby compromising the integrity of the information processed and stored by the university.

The aforesaid information breach scenario was avoidable and the impact of the breach minimised if the attacked entity/institution protected all the critical data and information under a sound information security management system programme design to constantly assess, monitor and review its IT risks, strategy, policies, and procedures. The study therefore attempts to review the extant laws and legislations designed by the Nigerian government to help Institutions of Higher Education in Nigeria to effectively reduce the incidence of information security breaches and incidents on its information assets, reduce their cyber risk exposure, and indeed financial and reputational losses that may arise from a breach. This is against the backdrop of global concerns and interest in information security management. The purpose of this study is; (1) Evaluate the impact of information security threats and attacks in institutions of higher learning; (2) Find out existing information legislation and its effect on information security; (3) Examine the factors militating against effective information security management in institutions of higher learning in Nigeria; (4)

Proffer solution on how to improve information security in higher institutions of learning in Nigeria.

2. Materials and Methods

2.1 Types of research

Research strategies in general terms are a set of action plans by which a researcher addresses the research questions and achieves the set research goals (Saunders et al., 2019). Multiple cases have been chosen for this study to enable comparisons between the multiple cases and to provide an opportunity to replicate the research findings across the cases and other institutions of higher education in Nigeria. Refers to this as literal replication. This study adopted a combination of the Archival and documentary research, and Case study research (multiple case study) strategies for the secondary and primary research data respectively for the reasons below. (a) The study depended on collecting and analysing secondary data from credible sources to address certain of the research objectives and questions to understand the current situation and establish themes and theory using the archival and documentary research strategy. (b) The case study strategy has been selected for the exploratory side of this research study through the administration of interviews on the participants selected.

2.2 Research Subjects and Objects

This study examines information security at the institutions level and therefore the unit of analysis for this study was Institutions of Higher Education while the unit of observation was done at individual level of observation. The research participants for this study were drawn from the staff members of IT/IS department or similar function within the case studies (Systems Engineers, Network Engineers, Network Managers, IT support Managers, Information systems Managers, Information Systems Administrators, Directors and Assistant Directors of IT, ICT Technical committee members, Chief information officers and Information security analysts). Only individuals whose job function falls within the job functions specified above were recruited for this study irrespective of their age, gender, religion and ethnicity. The study population criteria were not defined to infer that only individuals within the listed job functions are knowledgeable on the subject matter but for manageability and ensuring that only individuals with practical knowledge of the research subject were recruited to provide reliable data to achieve the study objectives and answer the study questions. The population size for this study was twelve individuals who are within the job functions specified above across the three institutions under study.

Purposive sampling a non-probability sampling technique was used to recruit participants for this study. Sangestani & Khatiban, (2013) explained that researchers use purposive sampling to select participants in a deliberate manner using specific individual characteristics of the study subject matter while (Creswell, 2014; Ishak & Bakar, 2014), maintained that purposive sampling is very appropriate for case study research. Purposive sampling provides researchers the opportunity to identify suitable participants who can provide the needed data to address the research questions and objectives (Smith et al., 2013). The choice of purposive sampling was to ensure that participants that are knowledgeable and have a sound understanding of the research subject area were selected. A sample size of between 10 and 20 participants is appropriate for qualitative research theme confirmation (Hanson et al., 2011).

2.3 Data Types and Sources

The types of data used in this research are primary data and secondary data. Primary data consists of: the results of interviews with school community data sources consisting

of the principal, deputy curriculum 4 subject teachers, secondary data obtained from documentation studies of learning plans (teaching modules) and assessment data.

2.4 Data collection technique

Data collection for this study was in two parts. Part one is the collection of secondary data from reputable sources discussed in the secondary data collection section below, while part two is the collection of primary data from participants from the case studies using semi-structured phone and zoom interviews.

This study harvested secondary data from the sources listed in Table 1, using the archival and documentary strategy to support the study objectives and address some of the research questions. As affirmed in Almalki, (2016); Creswell, (2014), the beginning of most research is the investigation to discover already existing knowledge and what remains to be learned about a topic through already published literature and previously collected data. The exploratory part of this study as employed secondary data to establish clear understanding of the topic through already published work and previously collected data. Secondary research data is data collected by another researcher, government agency, non-government agency and other organizations that a researcher can obtain for their own research (Matthews & Ross, 2010; Saunders et al., 2019).

Table 1. Selected Sources of Secondary data and applicability to the research work

Secondary data source	Nature of data	Applicable area of the study	Applicable to the research question
Verizon 2017, 2018, and 2019 Verizon and 2018 data breach digest	compiled	Data breaches in education, actors, motives, pattern and affected assets, common threats to information security	RQ 1 literature Review
Bitsigt insight report 2016	Compiled	Understanding of ransomware enabled attack in education and establishing trends in ransomware in education	RQ 1
Privacy rights clearinghouse Chronology of data breaches	Raw	Data breaches in US universities. Understanding trends in education sector cyberattack and literature review	RQ 1
Journal articles published between 2010 and 2020 on information security in higher education cyber threats, etc.	Compiled	Literature review and other areas of the research work	RQ 2,3,5

The data that has been collected is then analyzed. Data analysis was carried out descriptively. The steps taken to analyze and interpret qualitative research data are, (1) preparing and organizing the data; (2) explore and code the database; (3) describe findings and form themes; (4) represent and report findings; (5) interpret the meaning of the findings; and (6) evaluate the accuracy of the findings.

The primary data for this study was collected using semi-structured interviews. Phone and online zoom interview was adopted as against face-face interviews. Semi-structured interview is well suited for this study research purposes (exploratory and evaluative) and research questions (Saunders et al., 2019). The interviews were conducted

institution by institution and there was a two days interval between each institution interview to allow for understanding of the themes and patterns being revealed from the interviews to avoid data overload.

Participants who fall within the research population from the case study institutions were administered semi-structured interviews in English and Hausa Language using phone calls and zoom to understand their institution environment and the research questions as it affects their institution. The interview began with a general introduction after which note taking and recording was done. Seven participants were interviewed out of the twelve participants originally invited for participation. Six of the interviews were through Zoom and one through phone call. Each interview lasted between 10-45 minutes.

2.5 Data Analysis Techniques

This section discusses the data analysis method employed to carry out qualitative analysis of the primary data and secondary data. Qualitative research employs an interactive data collection and analysis thereby allowing the researcher to identify important themes, patterns and relationships as the data is collected (Creswell, 2014; Matthews & Ross, 2010; Saunders et al., 2019). The primary data was analysed using "Content Analysis" following the process and procedure outlined in Figure 1. below while the secondary data was analysed using exploratory analysis.

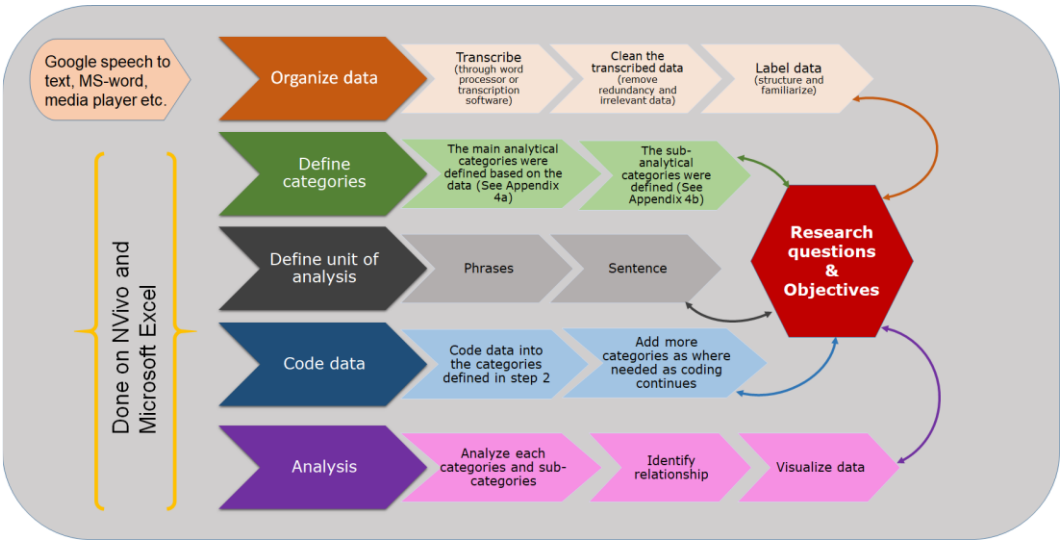

Figure 1. The adopted primary data analysis process and procedure (Saunders et al., 2019)

The analysis of the semi-structured interview qualitative data was done through QSR NVivo for Windows Release 12 (426), a software for qualitative data analysis. The NVivo software is loaded with different functions such as management of interview and project data coding, data categorization, classification, cases, relationship, notes and memos, query, visualization and reports. The use of such data management software as NVivo is becoming a norm in qualitative research as it makes it easier to organize large qualitative data sets thereby making the analysis process transparent and enriched.

The process of the analysis in NVivo began by installing the software, creating the project. Once the project was created, we began by creating Cases (respondents). Case classifications (Demographics). Importing the transcribed respondent's transcript into the file data management, creating the main Codes and sub code categories. The imported transcripts were linked to their respective Cases created earlier in the process and the demographics data such as education level, institution type, job role etc. was applied to the Cases based on the data the respondents provided during the interview. The final step of analysis was going through the imported interview transcripts one after the other and categorizing text statements into the different Code categories. It was after all the interview

data has been categorized that different results and queries are then spooled from the project.

3. Results

3.1 Participant profile

The data classifications (Demographics), importing the transcribed respondent's transcript into the file data management, creating the main Codes and sub code categories, namely; The participant profile as presented in Table 2, participants institution type presented in Figure 2, Participants Institutions ownership structure presented in Figure 3, and Participants Educational Qualification presented in Figure 4.

Table 2. Participants profile

Education level	Institution type	Number of years in the institution	Job role
MSc	University	11 years & above	Chief information officer
BSc	University	6-10 years	Information Security professional
MSc	University	11 years & above	ICT Director
MSc	University	0-5 year	Information system specialist
HND	University	0-5 year	Network administrator
PhD	University	11 years & above	ICT director
MSc	University	6-10 years	Computer science/Security lecturer (ICT Committee)

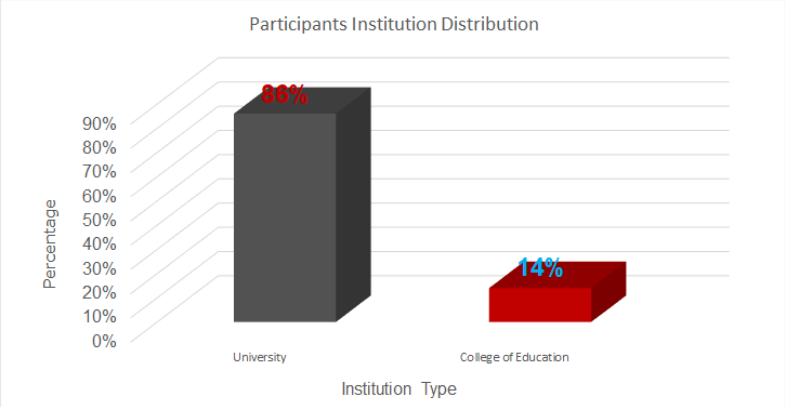

Figure 2. Participants institution type

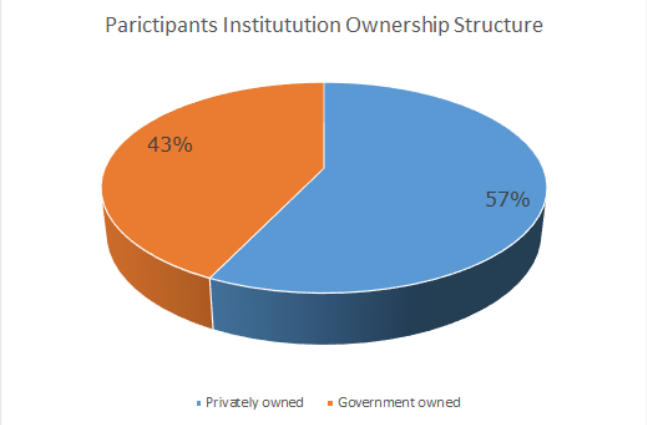

Figure 3. Participants Institutions ownership structure

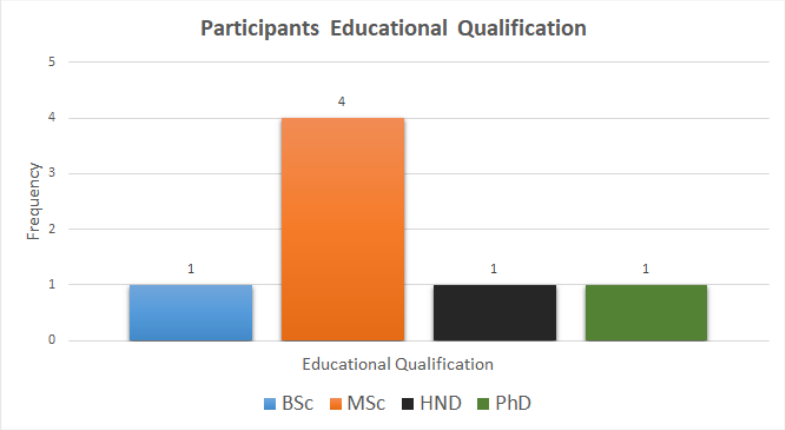

Figure 4. Participants Educational Qualification

3.2 Information security environment, culture and legislation (Interview question 5 and 6)

This section discusses the findings on environmental factors, culture and legislation and their impact on the institution's information security program.

3.2.1 Environmental and cultural factors

The findings made here shows that some of the factors were limiting while others were helpful to the information security endeavours of the institutions. The results of the environmental and cultural factors are presented in Figure 5. Budgetary constraints account for 21% of the limiting factors, followed by lack of top management support at 17%, while internal politics and lack of security professionals account for 13% respectively. The lack of training, which could be related to budget constraints and internal politics, accounts for 8% and finally government interference and location of the institution, which could have influenced the lack of security professional, represents 4% of the limiting factors.

To show the seriousness of the budgetary constraints factor, five out of the seven (71%) interviewed participants spoke about it as the biggest limiting factor, while lack of top management support featured in four out of the seven (57%) respondents. The government interference factor is majorly associated with the government owned institutions although it could affect the privately owned institutions in terms of policies and legislations. Two factors that contributed to the success of information security practices in one of the case study institutions are; availability of experienced security professionals in the institution 13% and well-informed user community 8%. Two of the participants emphasized the importance of the informed user community on the success of their security program even though they believe a lot still need to be done in this regard.

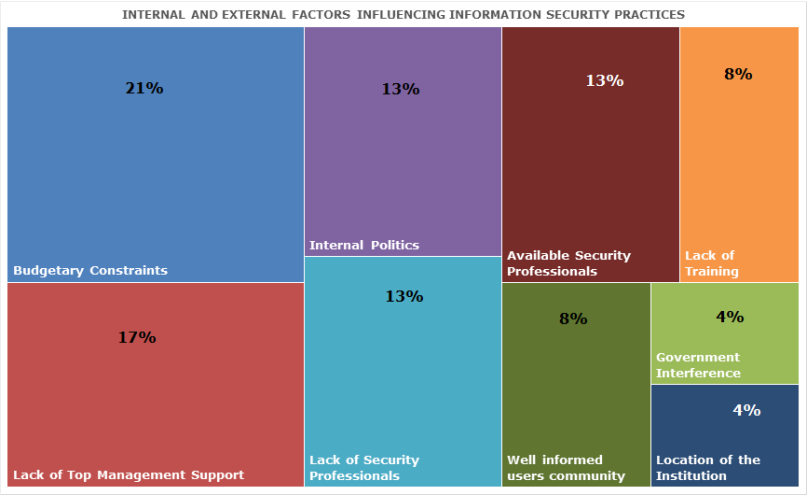

Figure 5. Internal and external factors influencing information security practices in IHEs

3.2.2 Legislations effect on information security

On the legislation side, the interview responses in Figure 10, shows that none of the case study institutions was abiding by the requirement of any of the information security legislations in the country. Three of the participants (43%) claimed they were aware data protection legislation existed in Nigeria. IHEs Adherence to information security legislations presented in Figure 6.

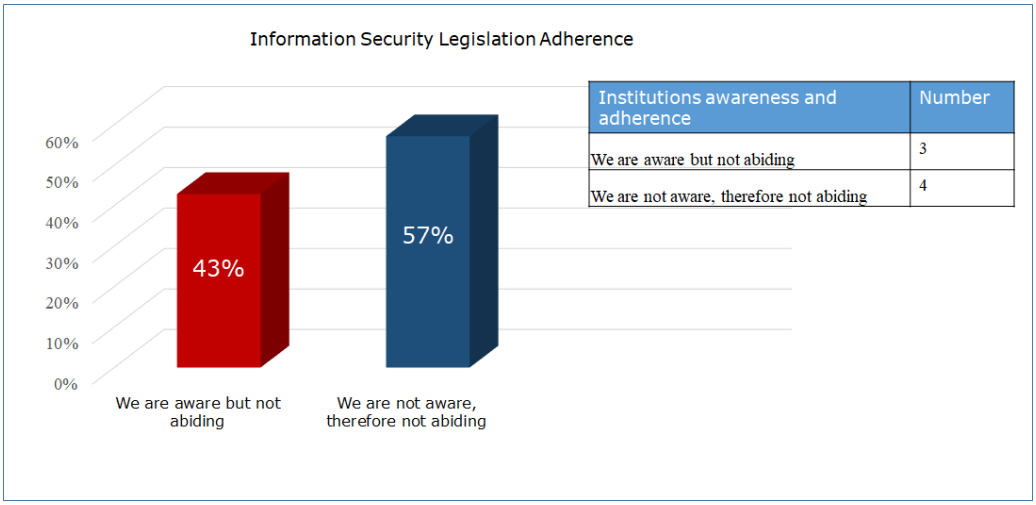

Figure 6. IHEs Adherence to information security legislations

3.3 RQ 1: What is the impact of data breach on Institutions of Higher Education when it occurs?

To address this research question, data from documentary research and qualitative semi-structured interviews were combined. The researcher started by seeking to understand the kind of data IHEs processes and stores that could be of interest to attackers. Table 3 below shows the Institutions of Higher Education attack targeted data. The top three targeted data revealed by the primary data are personal, financial and academic data with 23% each. The secondary data also shows that personal data top the list of the Verizon compromised data in the three years (2017-2019) under review with 56%, 72% and 55% respectively. The interview respondents indicated that all the three case study institutions had experienced a cyber-attack in the last Four years with yet to be quantified impact. Unfortunately, respondents from two case study institutions could not explain the impact the experienced cyber-attack had on their respective institution.

The identified impact of the successful attack on the third institution as presented in Ranges from financial loss, loss of public trust and reputational damage at 33% respectively. Although the respondents were not able to give the specific monetary value, they claimed it was huge. The reputational damage and loss of public trust, which cannot be quantified literally could also result in financial loss as the institution may lose public investment and may also experience decline in enrolment. According to Serianu, (2016) the yearly cost of cyber-attacks in Africa is $859 million broken into $537m indirect cost and $358m direct cost. The impact of a successful cyber-attack on an institution is both huge and unimaginable as has been revealed. The identified Attack targeted data can be seen in Table 3 and Identified attack Impact on the IHEs presented in Table 4.

Table 3. Identified Attack targeted data

Respondents identified attack target				Verizon unidentified attack target		
IHEs Attack targeted data	Respondents	Target data frequency	Target data percentage	2017	2018	2019
Academic data	3	3				
Health data	3	3				
Internal secrets	2	2				
Personal data	2	2	23%	56%	72%	55%
Credential	3	3		8%		35%
secrets				27%	14%	
	n=4	n=3				

Table 4. Identified attack Impact on the IHEs

Impact of attack			
	Respondents	Impact frequency	Impact percentage
Financial loss	2	2	33%
Loss of public trust	2	2	33%
Reputational damage	2	2	33%
	n=4	n=6	

3.4 RQ2: Is present legislations effective in addressing information security threats?

In the attempt to address this research question, it was discovered that only few of the respondents were aware of information security legislation in Nigeria and the three case study institutions were not abiding by the information security legislation. Higher education institutions as entities operating in Nigeria and processing and storing data of data subjects, and making use of technology are required to abide by the Nigeria Data Protection Regulation 2019 and the Cybercrime Prohibition, Prevention Act of 2015. It is expected that the information security plans, policies and strategy of the Institutions of Higher Education should be an offshoot of the two legislations mentioned above even though both legislations are quite recent with the oldest about five years old.

As already mentioned, the institutions that had experienced a breach or security incident never did notify the affected users and the regulatory agencies. This is because the legislation did not make it mandatory for data subjects to be notified when their data is compromised and no penalty for non-compliance was mentioned therein. According to Serianu, (2016), the absence of practical regulatory guidance from industry regulators and government is fuelling the poorly implemented security controls that are very hard to enforce.

3.5 RQ 3: What mechanism can be put in place to improve knowledge and understanding of information security in higher institutions?

This research question was intended to understand the level of user awareness in terms of information security in the institutions and how user awareness could be used alongside other technical controls to improve the Institutions of Higher Education exposure to breaches and incidence. Two of the interview questions were used to address this question. The responses received from the respondents as shown in table 5 shows that the state of information security awareness in the institutions is poor as 67% of the responses showed that the institutions does not have an information security awareness program in place, while 22% of the responses showed some level of awareness through email, and 11% through workshop and seminar. Al-Daeef et al., (2017), reemphasized the

known fact of human beings being the weakest link in the information security circle hence the need for improved user awareness. The respondents identified state of Information security awareness presented in Table 5.

Table 5. The respondents identified state of Information security awareness

Information security awareness program Awareness method	Respondents	Frequency of method	Percentage of method
Email campaign	2	2	22%
No information security awareness program in place or under development	6	6	67%
Seminars and workshop			11%
	n=7	n=9	

Institutions of Higher Education depending on technical measures alone cannot guarantee the needed level of security, as some security incidents like social engineering are hard to prevent or detect by technology. Awareness is therefore required to fortify this weakest link. The information security program will suffer a major setback if the users' community are not cyber-aware through education and awareness training (seminars, workshops, posters, newsletters). Phishing attacks have succeeded thus far because users are unaware of the threats, the organizational policy and cybercriminals have become more technically sophisticated (Desetty et al., 2024). Chu & So, (2020); Hagen et al., (2008) found that the success of IT security measures is heavily dependent on the emphasis the organization placed on information security awareness. Hina & Dominic, (2016) noted that though universities document their information security requirements in form of information security policies (ISP) and distributed to end-users through emails and network alerts, there is still a lot of doubt to the effectiveness and wholeness of the ISP because they are not delivered through dependable security education, training and awareness programs.

3.5 RQ 4: Is present legislations effective in addressing information security threats?

In the attempt to address this research question, it was discovered that only few of the respondents were aware of information security legislation in Nigeria and the three case study institutions were not abiding by the information security legislation. Higher education institutions as entities operating in Nigeria and processing and storing data of data subjects, and making use of technology are required to abide by the Nigeria Data Protection Regulation 2019 and the Cybercrime Prohibition, Prevention Act of 2015. It is expected that the information security plans, policies and strategy of the Institutions of Higher Education should be an offshoot of the two legislations mentioned above even though both legislations are quite recent with the oldest about five years old.

As already mentioned, the institutions that had experienced a breach or security incident never did notify the affected users and the regulatory agencies. This is because the legislation did not make it mandatory for data subjects to be notified when their data is compromised and no penalty for non-compliance was mentioned therein. Acording to Serianu, (2016) the absence of practical regulatory guidance from industry regulators and government is fuelling the poorly implemented security controls that are very hard to enforce.

4. Discussion

4.1 Analytical Review of the Nigerian Data Protection Framework

In Nigeria, the entire relevant laws and legislation over time stem from our colonial, post-colonial and military histories. This validates the preponderance of state-sanctioned surveillance aimed at regime protection and suppression of dissent voice as part of statecraft (Roberts et al., 2021). More often than not the justifications for surveillance and intelligence gathering are rooted in national security, preventing or investigating crime, protecting and safeguarding economic well-being, and public emergency or safety interests (Roberts et al., 2021; Serianu, 2016). The stark reality however is that this has been the tool used by the Nigerian state to gather purposive intelligence, intimidate the hapless populace, opponents, critics, and leaders of civil society organizations who challenge misgovernance (ibid). Every individual has a right to privacy, as do companies and other institutions in postmodern society. This right varies widely across countries around the world (Nte et al., 2022; Romansky & Noninska, 2020) The notorious state institutions that undertake these tasks are; the Department of State Security (DSS), the Defence Intelligence Agency (DIA) and the National Intelligence Agency (NIA), established by previous military regimes and continue to function in military and despotic fashion as state appendages even under the current civilian rule (Ibid).

In Nigeria, there are documented cases of covert clandestine surveillance activities in contravention of the provisions of the constitution and the Laws of the Federal Republic of Nigeria such as the 2013 $40 million contract saga perpetrated by the Nigerian government by fragrantly awarding the contract to Elbit Systems- an Israeli firm with the mandate to intercept internet activities and invade the privacy of Nigerian citizens (Abdulrauf & Fombad, 2016; Emmanuel, 2013). The same goes for the Citizens Lab report when in 2020, maintained that the Nigerian Defence Intelligence Agency acquired cyber-espionage tools ostensibly to spy on the opposition voices in the country (Marczak et al., 2020). In recent times, the Terrorism Prevention Act (TPA), the Cybercrimes Act, and the Mutual Assistance in Criminal Matters Act (MACMA) are strategic legislations designed to significantly place citizens under surveillance and stands a great risk of being abused by the Nigerian state against dissent voices. Specifically, Section 26 of the TPA, regulates intelligence gathering, and provides that the Attorney General, Inspector General of Police, or National Security Adviser may direct a communication service provider to retain communication data for the purpose of preventing a terrorist act or prosecuting offenders under the Act (Terrorism Prevention Act (TPA), 2013 as amended Gazette A27, at s.26).

In the same manner, the Cybercrimes Act authorizes law enforcement officers to apply to a judge ex-parte for a warrant to intercept data in any computer system or computer network, as well as to use any technology to decode or decrypt any coded or encrypted data contained in a computer into readable text or comprehensible format (Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015, at s.45 (2) (e) and (f). Section 38(1) of the act also requires service providers to keep traffic and content data for two years, while law enforcement agents are given the authority to request data from service providers (ibid). Filling in the gap between the rapid escalation of cybercrime and Nigeria's cybersecurity measures and supporting laws, is a fundamental need (Nte et al., 2022; Okibo & Ochiche, 2014). Furthermore, more recently, the Mutual Assistance in Criminal Matters Act of 2019 allows for the exchange of surveillance information with other countries relating to the identification and location of criminal offenders; obtaining evidence; intercepting telecommunications; and converting electronic surveillance.267.

In the telecommunications sector, the Nigerian Communication Commission (NCC) is charged with the entire gamut of regulating all internet service providers and telecommunications companies in Nigeria, and it has issued actionable regulations and guidelines including requiring service providers to intercept communications, decrypt encrypted communications, and provide communications data to law enforcement agencies (Nigerian Communications Commission Act, LFN 2003, N.9 at s.4(i)). The

Nigerian Communications Regulations of 2019 grants the NCC the role of monitoring and enforcement powers and mandates that licensees shall keep records of call data under the Cybercrimes Act (Nigerian Communications (Enforcement Process, etc.) (Roberts et al., 2021). Regulations 2019, B 82 at reg. 8(1). The NCC also introduced the Lawful Interception of Communications Regulations in 2019, with a regulatory framework for lawful interception, collection, and disclosure of intercepted communications in Nigeria, and states that only authorized agencies, which are the Department of State Security, the Nigeria Police Force, and the Office of the National Security Advisor, may intercept communication data subject to obtaining a court order (Lawful Interception of Communications Regulations 2019 B105).

The regulation further mandates service providers to install capabilities that permit interception and prohibits network providers from providing services that cannot be intercepted and monitored (ibid). The CJEU has established that, while lawful interception of personal data may be required to ensure national security, the principles of proportionality and necessity must be considered. International standards have also been established to ensure that appropriate safeguards, such as judicial authorization, effective independent oversight, transparency, and user notification, are in place to limit access to intercepted information. In this regard, the TPA 2013, as amended, introduced safeguards such as requiring interception of communication data to be subject to a warrant signed by a judge, and such order must specify the length of time the service provider must retain the communication data. The Cybercrimes Act also provides that a law enforcement officer may apply ex-parte to a Judge for a warrant to obtain electronic evidence in a criminal investigation; however, unlike the TPA, the Act does not specify how long such data can be retained and does not limit law enforcement access. The MACM Act also includes safeguards, ensuring that interceptions are limited to serious criminal situations (Mutual Assistance in Criminal Matters, 2019).

In all of these attempts to provide for the protection of the rights of the citizenry, there are copious gaps resulting in inadequate data protection templates. While the TPA and Cybercrimes Act require a warrant before data can be intercepted, it does not specify a test of necessity or proportionality and instead gives the authorizing judge broad discretion to order surveillance measures (Roberts et al., 2021). There are also no requirements under the identified laws for subject notification and an independent supervisory mechanism. The cybercrimes Act also does not limit the type of law enforcement agencies that can intercept data and this has led to its abuse by different law enforcement agencies such as the Nigeria's Economic and Financial Crimes Commission (EFCC), which is notorious for conducting illegal raids and searches in the name of fighting against cybercrime (Adewumi, 2022). The Cybercrimes Act's provision for unrestricted access for law enforcement agencies to search any data contained in a computer network equally raises grave privacy and human rights concerns in terms of arbitrary abuse by law enforcement agencies (NITDA, 2019).

4.2 Conceptual Framework

This research work is based on the concept that campus information security programs depend on many variables (technical and non-technical) which must all be present for the security program to succeed and achieve the desired result as revealed in the collected data for this study. Campus Information Security conceptual can be seen in Figure 7. The framework consists of four dependent components namely: technology and people, environment, authority and decisions, policies and standards, culture, education and incentives. There are many technological solutions to information security such as identity and access management, firewalls, intrusion detection and prevention systems, endpoint security, environmental monitoring and protection systems, cryptography etc.

These technological solutions must be matched with the right personnel (people) to achieve the desired result (Calder & Watkins, 2015; Reddy & Reddy, 2023) The people must have clearly defined responsibilities. You may have noticed that EAD, CEI and TP all have the people factor. This is deliberate since the level of the people as it relates to the security program is different. The EAD have the approving and governance people (senior management and board level), CEI have the entire institution community people who must be information security-aware for the institution to be able to build an efficient cyber-aware culture. Lastly, TP has the personnel that administer and manages the security program. The information security program must be environment specific and therefore setting the environment variables is key to the success of the information security program. As mentioned in Calder & Watkins, (2015), ISO27002 recommends managers to actively support security in their organizations through "clear direction, demonstrated commitment, explicit assignment and acknowledgement of information security responsibilities".

ISO/IEC (2013) mandates organizations to determine the borders and applicability of its information security management system through its scope. Policies and standards are important elements of an information security program (Disterer, 2013). ISO27001 clause 5.2 requires top management of an organization to establish an information security policy that is specific to the organization characteristics, location, assets and technology with clearly defined objectives to protect the Confidentiality, Integrity and Availability (CIA) of the organization's information assets and data, scope, specific goals and responsibilities at minimum (Calder & Watkins, 2015). noted that while setting an information security policy may not be so straightforward, yet organizations must put the same in place to have a working information security program. The policy must be a living document through regular review and update to capture the current needs and trends.

The information security program will suffer a major setback if the institution's community is not cyber-aware through education and awareness training (seminars, workshops, posters, and newsletters). Phishing attacks have succeeded thus far because users are unaware of the threats, the organizational policy and cybercriminals have become more technically sophisticated (Desetty et al., 2024). The institution must therefore educate its user's community of its policies and the emerging threats as Almalki, (2016) noted that information security awareness can confidently influence employee compliance to the organization's security policies.

A study by Hagen et al., (2008); Nowicka et al., (2024) found that the success of IT security measures is heavily dependent on the emphasis the organization placed on information security awareness. To underscore the importance of information security awareness in institutions of higher education, Ramalingam et al., (2016) conducted a of survey of 17 Institutions of Higher Education in Oman where it was found that although 22% of the institutions had adopted some information security practices, 39% of the respondents were unaware of such security practices. The study further revealed that 71% of the respondents had encountered a security attack between 1 to 3 times, 13% had fallen victim to security attacks more than 10 times in a year. The security attacks resulted in 36% of the respondents losing personal data while 35% got the computer system completely crashed.

Furthermore, building a cybersecurity-aware learning community may require an incentives system for users who adhere to the institution's information security practices

and policies. According to August et al., (2014); Ukwuoma et al., (2022) had noted that while the traditional patching practice has not yielded the desired results to the software vendors and the users because even though the software vendors release patches to fix vulnerabilities well enough, most times the users do not apply the patches as they are released leaving the vulnerabilities in place to be exploited. The authors therefore proposed an incentives-based approach that could help improve the patching practices.

A popular article on the economics of information security, has stated that "security failures are caused at least as often by bad incentives as by bad design" (Anderson & Moore, 2006; Itanyi, 2022; Witbooi et al., 2020). Liang & Xue, (2013) argued that while the stick approach of punishment of defaulters may encourage minimal compliance from the people, the carrot approach of rewarding those who practice good security hygiene yields better results. The incentives system is an important component of the framework. As the institution punishes defaulters, it must also reward those who follow good security practices.

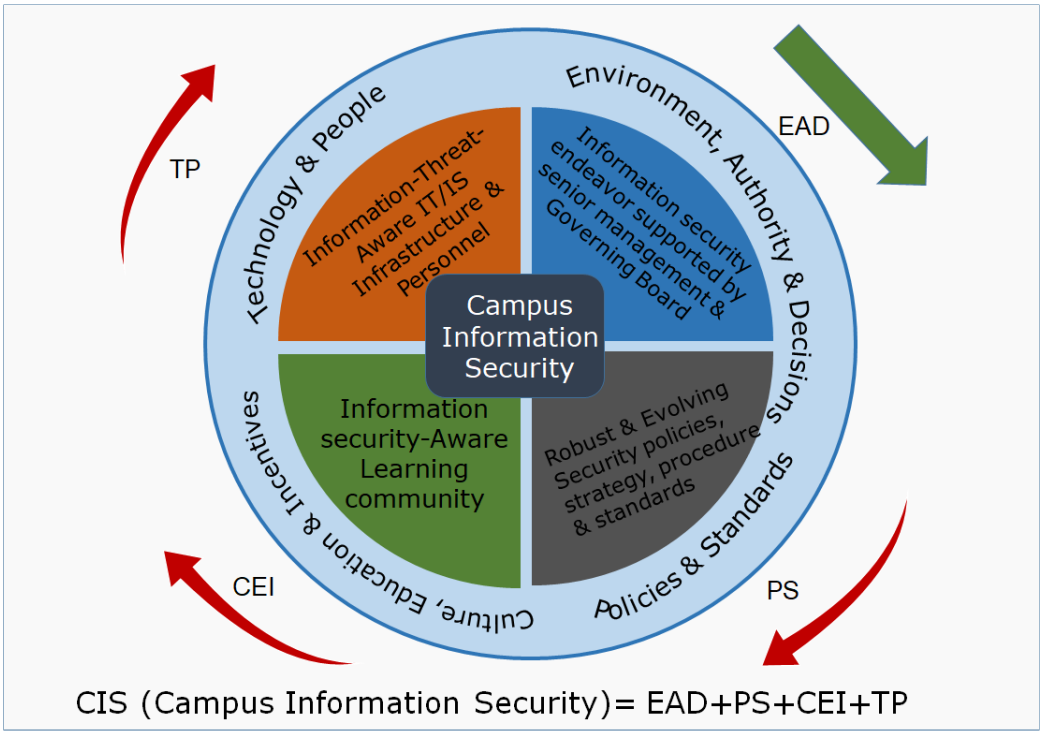

Figure 7. Campus Information Security conceptual

4.3 Summary

This study combined a mixed method approach of documentary and qualitative interviews to address the research topic and objectives. The documentary research showed that the education sector has been targeted by cybercriminals from both inside and outside sources with varying motives ranging from financial, espionage, fun etc. It was further revealed that the education sector processes and stores huge volume of personal, academic and research data that make them susceptible to such attacks. Furthermore, there are still lapses despite the various legislation on cybercrime and data protection. The qualitative interview data produced four themes: visibility and awareness of threats and sources, unstructured information security management, attacks, targets, motives and impact of information security breaches, and information security environment, culture and legislation.

4.4 Recommendations

Following from all that has transpired and the findings of this study, the following are recommended.

4.4.1 Recommendation for Institutions of Higher Education

In the previous part of this study, the conceptual framework for this study arising from the patterns revealed in the primary data was introduced. The case study institutions as already discussed in the summarized findings do not have any structured and documented IS program. The conceptual framework has been expanded to produce an integrated information security model in Figure 11, which can be used as a guide to the Institutions of Higher Education in developing their IS program.

The model comprises of two main components; the internal elements and the external elements (regulatory oversight function and industry standards and framework). The internal component comprises of four core elements and sub-elements. Furthermore, the model has four iterative security objectives: prepare and assess, detect, respond, heal and recover. The cybersecurity governance and regulatory oversight are very important components of this model as the primary data revealed lack of top management support and budgetary constraints as major hindrances to the Institutions of Higher Education Information Security program.

This proposed model, in itself, is the crucial recommendation for the Nigerian Institutions of Higher Education. This study found that the Nigerian Institutions of Higher Education were currently not doing enough and do not seem prepared to tackle the information security risks and threats facing it and the government and regulatory bodies have not provided any guidance for information security to the Institutions of Higher Education. This iterative and holistic model integrates an extensive array of elements for effective Information Security. Consequently, administrators and managers of Institutions of Higher Education could adopt the model as a conceptual map and guidance for the management of information security risks and threats facing their institutions. The Institutions of Higher Education urgently need to execute the four recommended priorities compiled in Figure 8 and Figure 9.

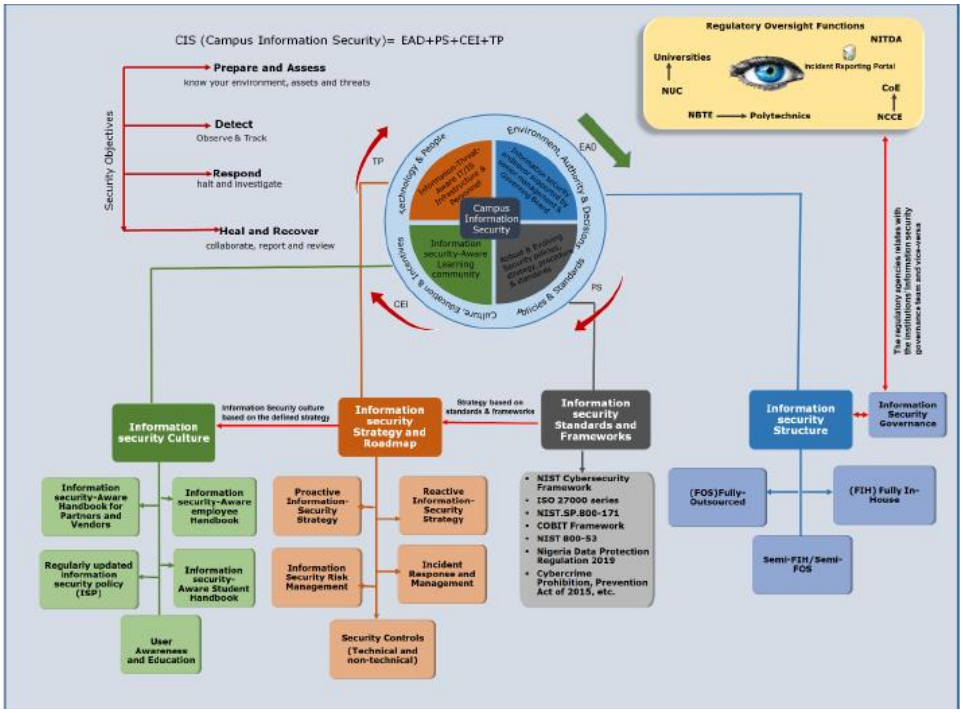

Figure 8. Proposed Integrated information security model for Institutions of Higher Education

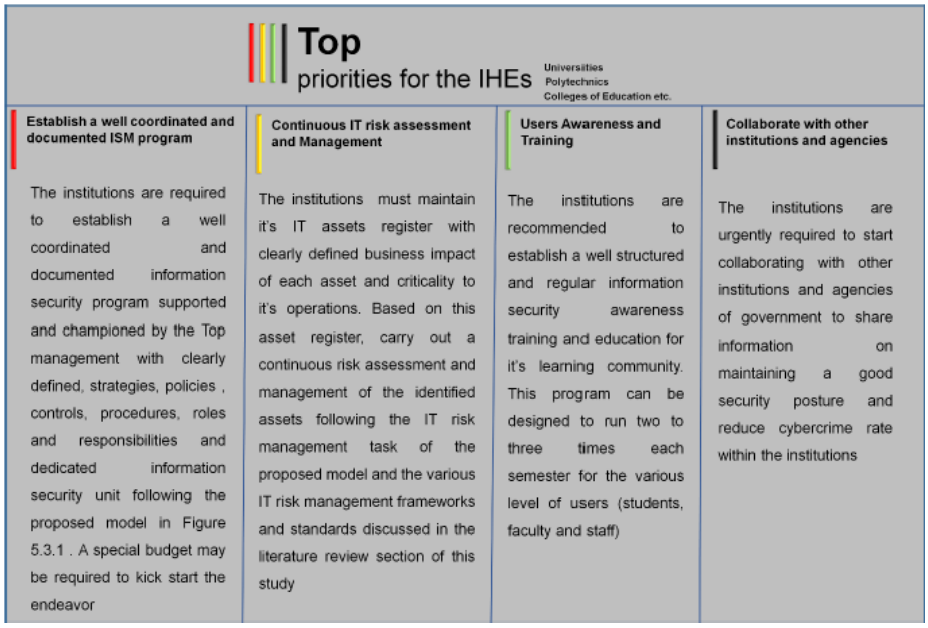

Figure 9: Institution of Higher Education Recommended Top Priorities

4.4.2 Recommendation for Regulatory Bodies and Government

The government through the regulatory bodies must play an active role in ensuring that the Institutions Higher Education take information security seriously through strategy, enforcement and monitoring. The recommended priorities for the government and regulatory agencies is presented in Figure 10.

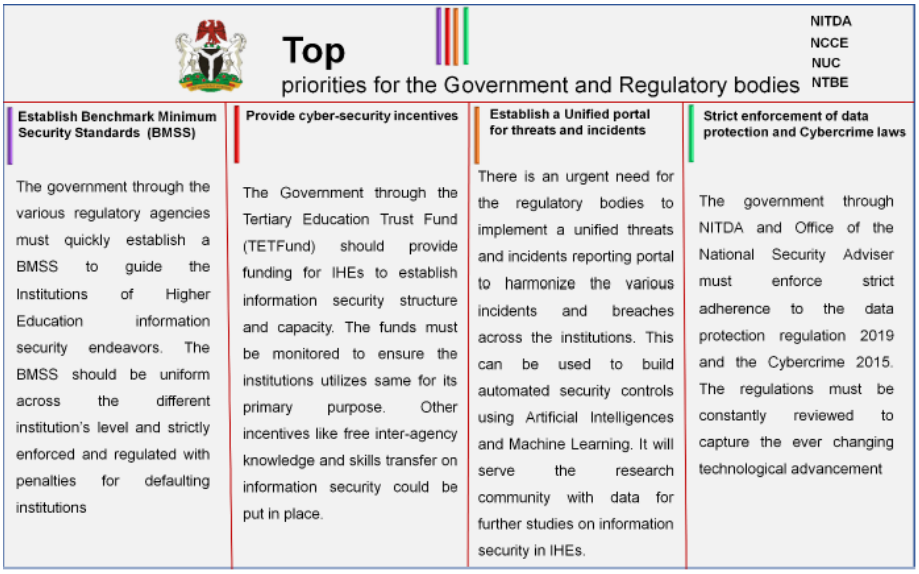

Figure 10. Recommended priorities for government and regulatory bodies

Finally, in information security discourses, the rule of law and accountability must be the pivot to establish good governance and development. Protecting the citizens' rights is a necessary requirement and this includes right to privacy and personal data. This however will require massive legal adjustments to create a congenial environment for information security of citizens. More so, the Nigerian judiciary must be independent to create the enhancement of data protection in Nigeria and it will also require a commitment by the Nigerian state to hold public and private institutions and entities accountable to laws that are enacted publicly, equally enforced, independently adjudicated, and consistent with international human rights norms and standards.

So far, Nigeria's current data protection legislation is a mere subsidiary legislation developed by a government agency without legislative oversight or approval. It is essentially a stopgap measure. It is therefore needful for the country to develop a comprehensive data protection framework with the appropriate parliamentary Acts based on local realities. There is a great need for Nigeria to establish a truly homegrown data protection framework that can be replicated in Sub-Saharan Africa. The development of comprehensive data protection legislation can only be accomplished through thorough and wide-ranging consultation with both local and international stakeholders bearing in mind that national interests must come first. In all, it should be noted that information security threats in institutions of higher education in Nigeria should be taken quite seriously as they are a critical segment of information security cycle. It is the gateway to the national information security architecture and management.

5. Conclusion

In conclusion, the aim of this study has been achieved largely through the enhanced understanding of the prevailing legislations on Information Security in Institutions of Higher Education in Yola that has been demonstrated throughout this study. The methodology adopted for this study makes the findings trustworthy for future study attempting to solve the problem of Information Security in higher education in Nigeria and beyond. The area of information security in Institutions of Higher Education in Nigeria and Sub- Sahara Africa has many opportunities for researchers, security industries and security professionals to explore. Collaboration and information sharing in the area of information security among the Institutions of Higher Education will go a long way to strengthen information security in the institutions.

Authors Contribution: NDN; VAT; AR, all authors contributed to the research and writing of the article (methodology, conducting the research and writing original article, field data collection, data analysis, and revision)

Conflict of Interest: The authors declare no conflict of interest.

Acknowledgements: The author thanks to Department. of Intelligence and Security Studies & Provost, College of Management and Social Sciences, Novena University

6. References

Abdulrauf, L. A., & Fombad, C. M. (2016). The African union's data protection convention 2014: A possible cause for celebration of human rights in Africa? *Journal of Media Law*, *8*(1), 67–97. https://doi.org/10.1080/17577632.2016.1183283

Adewumi, A. (2022). Adequate protection': An analysis of Nigeria's data protection laws within an emerging global data protection framework. In *Braz Dent J.* (Vol. 33, Issue 1). https://dspace.library.uvic.ca/server/api/core/bitstreams/c4f94bc6-e987-4375-82fa-76bb3ffba2db/content

Al-Daeef, M. M., Basir, N., & Saudi, M. M. (2017). Security awareness training: A review. *Lecture Notes in Engineering and Computer Science*, *2229*, 446–451. https://www.iaeng.org/publication/WCE2017/WCE2017_pp446-451.pdf

Almalki, S. (2016). Integrating Quantitative and Qualitative Data in Mixed Methods Research—Challenges and Benefits. *Journal of Education and Learning*, *5*(3), 288. https://doi.org/10.5539/jel.v5n3p288

Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, *314*(5799), 610–613. https://doi.org/10.1126/science.1130992

August, T., August, R., & Shin, H. (2014). Designing user incentives for cybersecurity. *Communications of the ACM*, *57*(11), 43–46. https://doi.org/10.1145/2629487

Bitsight. (2016). *Bitsight insights report the rising face of cyber crime: ransomware*.

https://cdn2.hubspot.net/hubfs/277648/Insights/BitSight_Insights_-_The_Rising_Face_of_Cyber_Crime_Ransomware.pdf

Calder, A., & Watkins, S. (2015). *IT governance: An international guide to data security and ISO 27001/ISO 27002*. IT Governance Publishing. https://www.torrossa.com/it/resources/an/5813750

Chu, A. M. Y., & So, M. K. P. (2020). Organizational information security management for sustainable information systems: An unethical employee information security behavior perspective. *Sustainability (Switzerland)*, *12*(8), 1–25. https://doi.org/10.3390/SU12083163

Creswell, J. W. (2014). *Research design: qualitative, quantitative, and mixed methods approaches 4th ed.* https://books.google.co.id/books?id=4uB76IC_pOQC&printsec=copyright&hl=id#v=onepage&q&f=false

Desetty, A. G., Jangampet, V. D., & Pulyala, S. R. (2024). Phishing attacks: Evolving techniques, emerging trends , and countermeasure strategies. *International Journal for Innovative Engineering and Management Research*, *9*(12), 985–991. https://www.researchgate.net/publication/376645699_Phishing_Attacks_Evolving_Techniques_Emerging_Trends_and_Countermeasure_Strategies

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, *4*, 92–100. https://doi.org/10.4236/jis.2013.4201

Elhabashy, A. E., Wells, L. J., Camelio, J. A., & Woodall, W. H. (2019). A cyber-physical attack taxonomy for production systems: a quality control perspective. *Journal of Intelligent Manufacturing*, *30*(6), 2489–2504. https://doi.org/10.1007/s10845-018-1408-9

Emmanuel, O. (2013). *EXCLUSIVE: Jonathan awards $40million contract to Israeli company to monitor computer, Internet communication by Nigerians*. PREMIUM TIMES. https://www.premiumtimesng.com/news/131249-exclusive-jonathan-awards-40million-contract-to-israeli-company-to-monitor-computer-internet-communication-by-nigerians.html

Garba, A., Musa, M. A., & Othman, S. H. (2020). A Study on cybersecurity awareness among students in Yobe: A quantitative. *Et International Journal on Emerging Technologies*, *11*(5), 41–49. https://d1wqtxts1xzle7.cloudfront.net/64160387/A_Study_on_Cybersecurity_Awareness-libre.pdf?1597243536=&response-content-disposition=inline%3B+filename%3DA_Study_on_Cybersecurity_Awareness_Among.pdf&Expires=1735459622&Signature=NpaJtz~H0vpUprRAY27~EK60U2U

Grajek, S. (2018). Top 10 IT issues, 2018: The remaking of higher education. In *Educause Review* (Vol. 53, Issue 1). https://er.educause.edu/-/media/files/articles/2018/1/er181100.pdf%0Ahttps://er.educause.edu/articles/2018/1/top-10-it-issues-2018-the-remaking-of-higher-education

Hadzhikoleva, S., Orozova, D., Andonov, N., & Hadzhikolev, E. (2019). Generalized net model of a system for quality assurance in higher education. *AIP Conference Proceedings*, *2172*(January 2022), 1–10. https://doi.org/10.1063/1.5133515

Hagen, J., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, *16*(4), 377–397. https://doi.org/10.1108/09685220810908796

Hammar, R. K. R. (2022). Common law approaches to addressing cybercrime and adolescent bullying in Indonesia: Focusing on accountability and protection in the digital age. *International Journal of Cyber Criminology*, *16*(2), 162–174. https://doi.org/10.5281/zenodo.4766573

Hanson, J. L., Balmer, D. F., & Giardino, A. P. (2011). Qualitative research methods for medical educators. *Academic Pediatrics*, *11*(5), 375–386. https://doi.org/10.1016/j.acap.2011.05.001

Hasan, R. (2023). Understanding the perception and awareness of education technologies' privacy and security issues. In *Proceedings on Privacy Enhancing Technologies* (Vol. 2023, Issue 4). Association for Computing Machinery. https://doi.org/10.56553/popets-2023-0110

Hina, S., & Dominic, D. D. (2016). Information security policies: Investigation of compliance in universities. *2016 3rd International Conference on Computer and Information Sciences, ICCOINS 2016 - Proceedings, August 2016*, 564–569. https://doi.org/10.1109/ICCOINS.2016.7783277

Ibrahim, Y. A., Ishaya, A. O., Yusuf, M., Nancy, I., Bijik, H. A., & Aiyedogbon, S. F. (2024). Cybersecurity and cybercrimes in Nigeria: An overview of challenges and prospects. *International Conference on Science, Engineering and Business for Driving Sustainable Development Goals, SEB4SDG 2024, April*, 1–7. https://doi.org/10.1109/SEB4SDG60871.2024.10630301

Ishak, N. M., & Bakar, A. Y. A. (2014). Developing sampling frame for case study: Challenges and conditions. *World Journal of Education*, *4*(3), 29–35. https://doi.org/10.5430/wje.v4n3p29

ISO/IEC. (2018). *Information technology — Security techniques — Information security management systems — Overview and vocabulary*. ISO/IEC 27001:2022/Amd 1:2024. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27000:ed-5:v1:en

Itanyi, N. (2022). The emerging digital economy in Nigeria : sacrificing the protection of privacy and data of consumers on the altar of economic growth. *European Intellectual Property Review*, *44*(3), 172–180. https://pureadmin.qub.ac.uk/ws/portalfiles/portal/298456607/The_Emerging_Digital_Economy_in_Nigeria_Sacrificing_the_Protection_of_Privacy_and_Data_of_Consumers_on_the_Altar_of_Economic_Growth.pdf

Jacob, O. N., Solomon, A. T., & Jegede, D. (2020). University education policies in Nigeria: Challenges preventing the implementation and the ways forward. *Jurnal Sinestesia*, *10*(2), 66–85. https://sinestesia.pustaka.my.id/journal/article/view/54

Kraus, S., Durst, S., Ferreira, J. J., Veiga, P., Kailer, N., & Weinmann, A. (2022). Digital transformation in business and management research: An overview of the current status quo. *International Journal of Information Management*, *63*(December 2021). https://doi.org/10.1016/j.ijinfomgt.2021.102466

Liang, H., & Xue, Y. (2013). Ensuring employees ' IT Compliance: Carrot or stick ? *Information Systems Research*, *June 2013*, 1–16. https://doi.org/10.1287/isre.1120.0427

Longo, F., Padovano, A., & Umbrello, S. (2020). Value-oriented and ethical technology engineering in industry 5.0: A human-centric perspective for the design of the factory of the future. *Applied Sciences (Switzerland)*, *10*(12), 1–25. https://doi.org/10.3390/APP10124182

Marczak, B., Scott-Railton, J., Rao, S. P., Anstis, S., & Deibert, R. (2020). *Running in circles Uncovering the clients of cyberespionage firm circles*. https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

Matthews, B., & Ross, L. (2010). *Research methods: A practical guide for the social sciences. 1st ed.* Pearson Longman. https://books.google.co.id/books/about/Research_Methods.html?id=7s4ERAAACAAJ&redir_esc=y

Mitchell, O., & Osazuwa, C. (2023). Confidentiality, integrity, and availability in network systems: A review of related literature. *International Journal of Innovative Science and Research Technology*, *8*(12), 1947–1955. https://doi.org/10.5281/zenodo.10464076

Mutual Assistance in Criminal Matters (Amendment) Act 2019, Pub. L. No. No.8 of 2019, XXXIX Official Gazette 1 (2019). https://laws.gov.ag/wp-content/uploads/2019/08/No.-8-of-2019-Mutual-Assistnce-in-Criminl-Matters-Amendment-Act-2019-No.-8-of-2019-final.pdf

NITDA. (2019). https://nitda.gov.ng/wp-content/uploads/2020/11/NigeriaDataProtectionRegulation11.pdf

Nowicka, J., Ciekanowski, Z., & Milewska, A. (2024). Information security management as the basis for the functioning of an organization. *European Research Studies Journal*, *XXVII*(Issue 3), 128–141. https://doi.org/10.35808/ersj/3427

Nte, N. D., Enoke, B. K., & Omolara, J. A. (2022). An evaluation of the challenges of mainstreaming cybersecurity laws and privacy protection in Nigeria. *Journal of Law and Legal Reform*, *3*(2), 246–266. https://doi.org/10.15294/jllr.v3i2.56484

Okeshola, F. B., & Adeta, A. K. (2013). The nature, causes and consequences of cyber crime in tertiary institutions in Zaria-Kaduna State, Nigeria. *American International Journal of Contemporary Research*, *3*(9), 98–114. https://www.aijcrnet.com/journals/Vol_3_No_9_September_2013/12.pdf

Okibo, B. W., & Ochiche, O. B. (2014). Challenges facing information systems security management in higher learning institutions: A case study of the catholic university of eastern Africa - Kenya. *Nternational Journal of Management Excellence*, *3*, 336-349. https://doi.org/10.17722/IJME.V3I1.133

Onohihu, S. C. (2022). The essence of government and perpetual insecurity in northern Nigeria 2016-2021. *International Journal of Social Sciences and Humanities Reviews*, *12*(1), 108–119. https://d1wqtxts1xzle7.cloudfront.net/91348889/798_2717_1_PB_2_-libre.pdf?1663776679=&response-content-disposition=inline%3B+filename%3DTHE_ESSENCE_OF_GOVERNMENT_AND_PERPETUAL.pdf&Expires=1735459937&Signature=gj73glVlozQpONPJ9SD0QQrMSElK0sy8elABh9oUVC3RqR

Ramalingam, R., Khan, S., & Mohammed, S. (2016). The need for effective information security awareness practices in Oman higher educational institutions. *Journal of Advances in Information Technology*, *3*(3), 1–7. https://doi.org/10.4304/jait.3.3.176-183

Reddy, G. nikhit., & Reddy, G. j. ugande. (2023). A study of cyber security challenges and its emerging trends on latest technologies. *International Journal of Innovative Research in Advanced Engineering*, *10*(06), 379–382. https://doi.org/10.26562/ijirae.2023.v1006.25

Roberts, T., Mohamed Ali, A., Farahat, M., Oloyede, R., & Mutung'u, G. (2021). *Surveillance law in Africa: A review of six countries Nigeria country report*. https://doi.org/10.19088/IDS.2021.059

Romansky, R. P., & Noninska, I. S. (2020). Challenges of the digital age for privacy and personal data protection. *Mathematical Biosciences and Engineering*, *17*(5), 5288–5303. https://doi.org/10.3934/MBE.2020286

Sangestani, G., & Khatiban, M. (2013). Comparison of problem-based learning and lecture-based learning in midwifery. *Nurse Education Today*, *33*(8), 791–795. https://doi.org/10.1016/j.nedt.2012.03.010

Saunders, M., Lewis, P., & Thornhill, A. (2019). Research methods for business students. In *Synthese* (Vol. 195, Issue 5). https://www.amazon.com/Research-Methods-for-Business-Students/dp/1292208783/ref=sr_1_2?dchild=1&qid=1614706531&refinements=p_27%3AAdrian+Thornhill+%2F+Philip+Lewis+%2F+Mark+N.+K.+Saunders&s=books&sr=1-2&text=Adrian+Thornhill+%2F+Philip+Lewis+%2F+Mark+N.+K

Serianu. (2016). Afica cyber security report 2016. In *European commissioon* (Issue November). https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf

Sigholm, J. (2013). Non-state actors in cyberspace operations. *Journal of Military Studies*, *4*(1), 1–37. https://doi.org/10.1515/jms-2016-0184

Smith, A. R., Colombi, J. M., & Wirthlin, J. R. (2013). Rapid development: A content analysis comparison of literature and purposive sampling of rapid reaction projects. *Procedia Computer Science*, *16*, 475–482. https://doi.org/10.1016/j.procs.2013.01.050

Sorokoumova, E. A., Puchkova, E. B., Cherdymova, E. I., & Temnova, L. V. (2021). The

risks and threats of digital educational technologies and products. *World Journal on Educational Technology: Current Issues*, *13*(4), 851–862. https://doi.org/10.18844/wjet.v13i4.6270

Ukhami, E. I., & Abdulsalam, D. (2024). Globalisation and national security: Perspectives on cybersecurity threats in Nigeria. *JOURNAL OF POLITICAL DISCOURSE*, *2*(2), 273–286. https://jopd.com.ng/index.php/jopdz/article/download/130/121/249

Ukwuoma, H. C., Williams, I. S., & Choji, I. D. (2022). Digital economy and cybersecurity in Nigeria. *International Journal of Innovation in the Digital Economy*, *13*(1), 1–11. https://doi.org/10.4018/ijide.292489

Vázquez-Cano, E., Parra-González, M. E., Segura-Robles, A., & López-Meneses, E. (2022). The negative effects of technology on education: A bibliometric and topic modeling mapping analysis (2008-2019). *International Journal of Instruction*, *15*(2), 37–60. https://doi.org/10.29333/iji.2022.1523a

Vilmer, J.-B. J., Escorcia, A., Guillaume, M., & Herrera, J. (2015). *Information manupulation a challenge for our democracies*. https://doi.org/https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf

Welc, D. (2019). Creating a Cybersecurity Strategy for Higher Education, 20 Mayo 2019 10 (2019). https://er.educause.edu/articles/2019/5/creating-a-cybersecurity-strategy-for-higher-education

Witbooi, E., Ali, K.-D., Santosa, M. A., Hurley, G., Husein, Y., Maharaj, S., Okafor-Yarwood, I., Quiroz, I. A., & Salas, O. (2020). Organized crime in the fisheries sector threatens a sustainable ocean economy. *Nature*, *588*(7836), 48–56. https://doi.org/10.1038/s41586-020-2913-5