Academic Journal Research
Homepage : https://journal.antispublisher.com/index.php/acjoure
Email : admin@antispublisher.com

e-ISSN : 3026-3085
ACJOURE, Vol. 3, No. 1, June 2025
Page 70-77

Operation of Cyber Security in Tertiary Institution in Nigeria: Problems and Way Forward

Bintu Yunisa[1], Safina Abdullahi Jantullu[2], Offia Ogochukwu Judith[3]
[1]Federal University Wukari, Nigeria
[2]Shehu Shagari College of Education, Nigeria
[3]Federal University Wukari, Nigeria

DOI : https://doi.org/10.51699/acjoure.v3i1.312

Sections Info

Article history:
Submitted: February 25, 2025
Final Revised: March 03, 2025
Accepted: March 07, 2025
Published: March 11, 2025

Keywords:
Cyber security
Tertiary institutions
Problems

ABSTRACT

Objective: *This study examines the challenges affecting the operation of cybersecurity systems in Nigerian tertiary institutions and proposes strategic solutions to enhance cybersecurity resilience in higher education.* ***Method:*** *This position paper is based on a comprehensive review of secondary data sourced from print and online publications, focusing on existing cybersecurity policies, infrastructure, and institutional frameworks.* ***Results:*** *The findings reveal critical challenges, including poor funding, inadequate cybersecurity infrastructure, weak cybercrime laws, lack of standardized national control, increasing cyber threats, shortage of cybersecurity professionals, decentralized network operations, rapid technological advancements, low awareness and training, and insufficient collaboration between institutions and government agencies.* ***Novelty:*** *This study highlights the urgent need for a structured national cybersecurity policy tailored for higher education institutions, emphasizing a multi-stakeholder approach involving government agencies, institutions, and cybersecurity professionals. The study recommends special funding allocations, enhanced infrastructure, regulatory policy frameworks, employment of cybersecurity experts, continuous professional training, and strengthened institutional-government collaboration to mitigate cybersecurity risks. The paper contributes to the ongoing discourse on cybersecurity in the education sector by advocating for an integrated, policy-driven approach to safeguarding digital assets in Nigerian tertiary institutions.*

INTRODUCTION

Tertiary education is an organized educational system that is consciously designed for manpower production, in-service training and national development. Tertiary education is an education that advances teaching, research and community services for national development. Tertiary education is an education industry that is meant for the production of manpower and national development via implementation of teaching, research and provision of community services [1]. Tertiary education, also known as higher education, refers to educational programs offered by universities, colleges, and other institutions beyond secondary education. It encompasses undergraduate and postgraduate studies, providing students with advanced knowledge, skills, and qualifications in their chosen field of study [2]. Ogunode and Mcbrown, tertiary education is an educational system that advances the implementation of the teaching programme, research programme and community service programme for the socio-economic, socio-cultural and technological development of a particular country. Tertiary education is defined as the teaching and learning processes that transpire following the completion of secondary education, culminating in the awarding of credits, certificates, diplomas, and degrees by universities, university colleges, polytechnics, community colleges, and analogous institutions. It is emphasized that this level of education may also encompass technical and vocational training. Tertiary education serves as a catalyst and driving force behind national objectives and aspirations, particularly when the quality of education is diligently upheld [3]. Tertiary education is characterized as an educational process encompassing teaching and learning specifically tailored for undergraduate and graduate students, which is initiated upon the successful conclusion of secondary education. This category of education may include vocational post-secondary institutions that culminate in a certificate, as well as higher educational institutions that confer degrees, despite the fact that the term is frequently employed interchangeably with higher education. Campbell and Rozsnyai further assert that tertiary education represents a formal, non-mandatory educational phase that succeeds secondary education. They conclude that tertiary educational institutions are distinctly differentiated from educational structures at primary and secondary levels [4]. Tertiary institutions are saddled with the responsibility of managing data which include students, staff and institutions' data or information. Tertiary institutions must prioritise enterprise-level cyber-security due to the large amount of sensitive data they hold, such as personal information, academic records, and financial details. Being a prime target for cybercriminals, a breach could result in severe consequences like identity theft and financial fraud. The management of cyber security operational system in the most Nigerian tertiary institutions appearing facing a lot of challenges. These challenges reduces the effectiveness and efficiency of the cyber security system in the various tertiary institutions in Nigeria. It is based on this, that this paper seeks to discuss the challenges facing the operation of cyber security system in the Nigerian tertiary institutions.

Literature Review. Cyber-security according to Ogunode, Akpakwu, & Ochai, is the consciously planned programme and policies measures that are technological inclined designed to protect personal data, institutional data, programme, resources from attack and damage from an unauthorized party. Cyber security is the best practices an individuals or institution adopt to reduce the risk of cyber-attack from intruder, insider or outsider from accessing confidential data. Cyber security's core function is to protect the devices the persons and institutions uses which include (handset, smartphones, laptops, tablets and computers), and the internet services access used that include online and at work - from attacks or damage. The aims of school cyber security includes; to protect and safe guide school confidential data from attacks; to protect students information from general public domain; to provide a strong security posture against attacks designed to access, alter, delete, destroy or extort school's or user's systems and sensitive data. Cybersecurity is an organized system for total protection data [5]. Cybersecurity is the practice of protecting internet-connected systems such as hardware, software and data from cyberthreats. It's used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems. Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users through ransomware or interrupting normal business processes. According to Kruse, Frederick, Jacobson, and Monticone in Muhammed cyber security is a set of strategies and processes for defending computers, networks, databases, and applications against assaults, illegal access, modification, or destruction. It can also play a vital role in the development of information technology and Internet services. The International Telecommunications Union [ITU] defines Cyber security as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment." Cybersecurity is the protection to defend internet-connected devices and services from malicious attacks by hackers, spammers, and cybercriminals [6]. Companies use the practice to protect against phishing schemes, ransomware attacks, identity theft, data breaches, and financial losses. Cybersecurity according to Nwachukwu [7], encompasses a set of policies, security concepts, tools, security safeguards, risk management approaches, guidelines, actions, best practices, training, assurance, and technologies that can be used to protect the cyber environment, organization, and user's assets. Organization and user assets include connected computing devices, personnel, applications, infrastructure, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security attempts to ensure the accomplishment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. From the above, cybersecurity in this paper is the individual' or institutional' practice and efforts to protect their computer systems and networks from theft, damage, or unauthorized access to data. Cybersecurity measures include implementing firewalls, antivirus software, and encryption protocols to prevent attacks from hackers, viruses, or malware [8]. Cybersecurity is the measures and actions designed to protect the computer, network and information from an unauthorized persons. The benefits of cyber security in educational institutions according to Ogunode, et al includes; 1) protection of school administration and business from cyberattacks and data breaches; 2) Protection of data and networks of school from attacks; 3) Prevention of unauthorized user access school cyber space; 4) Effective cyber security improves recovery time after a breach; 5) Protection for end users and endpoint devices of school from attacks; 6) It assist schools to safe guide students' data to adhere to educational laws and regulations; 7) Proper cyber security measures support stable academic work by protecting learning digital resources that are key to sustainable learning in schools; 8) Effective cyber security in schools improves confidence in the school's reputation and trust by parents, students, partners and education stakeholders. Also, the following are the objectives of Cyber-security according to Makeri, includes;. 1) to help people reduce the vulnerability of their Information and Communication Technology (ICT) systems and networks; 2) to help individuals and institutions develop and nurture a culture of cyber security; 3) to work collaboratively with public, private and international entities to secure cyberspace;4) to help understand the current trends in IT/cybercrime, and develop effective solutions; 5) availability; 6) integrity, which may include authenticity and non-repudiation and 7). Confidentiality.

RESEARCH METHOD

Secondary data was used in the paper. The secondary data were collected from print and online publication. Content analysis was employed for selection of literatures. Data Analysis on Challenges facing Operation of Cybersecurity in Nigerian Tertiary Institutions. Poor funding. Cyber security management is very capital intensive. It requires a lot of resources to be able to successfully manage cyber security programme. The cyber security management demands both human and materials resources that are very expensive to acquire. The poor funding of tertiary institutions in Nigeria has contributed to poor development of cyber security programme implementation in the various institutions. Due to funding from the government and poor support from the private institutions, many tertiary institutions managers have not be able to purchase necessary infrastructure facilities to support full development of cyber security programme or system in their respective institutions, lamented the poor funding of education especially the higher institutions in Nigeria has affected implementation of lourdable policies and programme that supposed to have aided the development of the institutions [9]. Musa poor funding of tertiary institutions responsible for low development of cyber security system in the institutions.

Inadequate security infrastructure

Inadequate cyber security infrastructural facilities in the tertiary institutions also contributing to slow development of cyber security system in the tertiary institutions in Nigeria. Cyber security infrastructure facilities are critical components in safeguarding computer systems and networks from malicious attacks. These facilities include hardware, software, and information systems that work together to protect valuable data and maintain the confidentiality, integrity, and availability of systems. With the increasing number of cyber threats and attacks, it is important for tertiary institutions in Nigeria to have access to adequate cyber security infrastructure facilities. The shortage of these facilities have affected the development of cyber security system in the tertiary institutions in Nigeria [10].

Lack of Strong Cyber Crime Laws

The weak laws and regulations refer to the lack of effective legal frameworks and policies that govern cybersecurity practices in the various tertiary institution in Nigeria. This can create an environment where cybercriminals can operate with impunity, knowing that there are few consequences for their actions. A study conducted by the

International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) found that "the absence of cybersecurity laws and regulations in Nigeria has contributed to the rise of cybercrime". Also, the lack of clear definitions and guidelines for cybercrime in Nigeria's legal system can make it difficult to prosecute cybercriminals. According to a report by the Global Cybersecurity Index (GCI), "Nigeria's legal framework for cybersecurity is weak and does not provide adequate protection for citizens and critical infrastructure" [11]. Many institutions do not have policies and regulation guiding staff and students on the activities of cyber securities in the institutions.

RESULTS AND DISCUSSION

Result

Lack of Standards and National Central Control: The lack of standards and national central control is another factor that appear to be contributing to low development of cybersecurity system in Nigerian tertiary institutions. It is impossible to develop a reliable and strong cyber security system without a centralized approach to cybersecurity nationally. There may be inconsistencies in the way that institutions and individuals approach cybersecurity management by adopting their policies and programme for implementation, leaving them vulnerable to cyber threats. According to a report by the Global Cybersecurity Index (GCI), "Nigeria does not have a national cybersecurity strategy or a national computer emergency response team (CERT), which means that there is no central point of coordination for cybersecurity activities" [12]. This lack of central coordination can make it difficult to respond effectively to cyber threats by institutions and can leave critical infrastructure and individuals at risk.

Increasing Cyber Threats: One of the major challenge to effective operation of cyber security in the Nigerian tertiary institutions is the high rate of cyber threat in Nigeria. Due to high rate of unemployment among the youths, the attacks on institutions cyber is high and this is a very big problem to manager of these institutions. Ukhami, and Abdulsalam, noted unemployment can contribute to cybersecurity threats in Nigeria. The lack of job opportunities can drive individuals to engage in cybercrime as a means of making a living. According to the National Bureau of Statistics (NBS) Nigeria's unemployment rate increased from 14.2% in Q4 2016 to 16.2% in Q2 2017 and 18.8% in Q3 2017. Again, in 2020 the National Bureau of Statistics, reported that "Nigeria's unemployment rate was 33.3% in the fourth quarter of 2020, which is one of the highest rates in the world". Maintained that employment prevents crime for some people under certain conditions and that employment and criminality relate to each in several ways not only at the aggregate level but also at the individual level. Nigeria has an unemployment problem. The unemployment rate has been identified as one of the factors responsible for youth involvement in cybercrime. Musa and Ogunode et al concluded that schools are often targeted with malware, phishing, and ransomware due to the wealth of personal data stored [13].

Lack of Expertise: Another problem hindering successful operation of cybersecurity programme and policies implementation in the Nigerian tertiary institutions is lack of adequate professionals in the field of cyber security that will help to manage their cyber facilities and space for the respective institutions. Many tertiary institutions no not have in their employment professionals and expertise in cyber security that will be in charge of cyber security management. The inability of these institutions to access adequate professionals in cyber security in their institutions has affected the development of cyber security system in the institutions. Musa noted that there is a shortage of staff with specialized cybersecurity knowledge.

Decentralised Networks: Another problem affecting operation of the cybersecurity system in the tertiary institutions is the decentralization of Networks to various faculties, department and units. Many tertiary institutions due to population have many faculties and department that cyber security must cover and these faculties, department and units must have special password for their staff and students. It requires a lot of resources to effectively monitor and manage this large cyber security operational links. The inability of the institutions to protect and monitor this network of operation is a very big problem in the Nigerian tertiary institutions. Musa and Nordlayer concluded that educational institutions often have spread out networks that are difficult to monitor and protect and this put the institutions and students in danger of attacks.

Discussion

Modern technological development. Cybersecurity challenges are becoming increasingly prevalent in tertiary institutions in Nigeria. The rapid advancement of technology has led to an increase in cyber-attacks, putting sensitive information at risk and causing disruptions to academic activities. There are modern technology been developed and are been accessed by different people. These technological devices have capacity to penetrate cyber space. The rise in cyber-attacks in tertiary institutions in Nigeria has been a major cause for concern in recent years. With the increasing use of technology in academic institutions, the vulnerabilities for cyber threats have also increased. This poses a significant challenge for the security of these institutions, as sensitive data and information are at risk of being compromised. Furthermore, the constantly evolving nature of cyber-attacks makes it difficult for institutions to keep up with the latest security measures. Hackers have become more sophisticated in their methods, making it challenging for institutions to stay ahead of them. This is especially true for smaller institutions with limited resources and budgets.

Lack of training. Lack of constant training for manager of cyber security department in the various tertiary institutions is also hindering the development of cyber security in the various institutions. The manger or officers managing the cyber security programme of the tertiary institutions needs training and retraining programme regularly because the high rate of technological advancement in the cyber space and management. There are many innovation and practices that are newly discovered that this cyber managers needs to know in order to effectively safe guide the institutions cyber space. The inability of these cyber manager to attend these training that will update their knowledge and technical know-how will affects the management of the cyber security system [14]. Musa noted that by staying up-to-date on the latest developments and implementing robust security measures, individuals and organizations can protect their sensitive information and maintain the integrity of their systems. One of the main challenges in cyber security for tertiary institutions in Nigeria is the lack of awareness and preparedness. Many institutions do not have proper training and resources to combat cyber-attacks, making them easy targets for hackers. This lack of preparedness also extends to students and faculty, who may not be knowledgeable about cyber threats and how to protect themselves [15].

Lack of collaboration between institutions and government agencies. Another challenge is the lack of collaboration between institutions and government agencies. In many cases, institutions do not report cyber-attacks or seek help from government agencies, which further exacerbates the problem. This lack of communication and collaboration hinders the development of effective strategies and solutions to combat cyber threats. Findings.The study revealed that poor funding, inadequate cyber security infrastructure facilities, lack of strong cyber-crime laws, lack of standards and national central control, increasing cyber threats, lack of expertise and professionals of cyber security, decentralized large networks operation, modern technological development, lack of awareness and training and lack of collaboration between institutions and government agencies.

CONCLUSION

Fundamental Finding : This study highlights the significant challenges impeding the effective operation of cybersecurity systems in Nigerian tertiary institutions, including inadequate funding, weak cybercrime laws, insufficient cybersecurity infrastructure, lack of standardized national control, and a shortage of skilled professionals. **Implication :** The findings underscore the urgent need for a structured, policy-driven approach to cybersecurity management in higher education, emphasizing institutional resilience, regulatory frameworks, and collaborative efforts between government agencies and academic institutions. Addressing these challenges is critical for safeguarding digital assets, ensuring data integrity, and fostering a secure learning environment. **Limitation :** This study primarily relies on secondary data, which may limit its scope in capturing real-time institutional cybersecurity challenges and practical interventions. Empirical studies involving primary data from key stakeholders would provide deeper insights. **Future Research :** Further research should explore the effectiveness of existing cybersecurity policies in Nigerian tertiary institutions, assess the impact of cybersecurity training programs on institutional security posture, and examine global best practices that can be adapted to enhance cybersecurity frameworks in the education sector.

REFERENCES

[1] I. A. Ajayi, A. Oluwasegun, O. Adeola, и Y. Adekunle, «Cybersecurity Governance in Nigeria: Legal Framework, Challenges, and Prospects», *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, т. 11, вып. 2, сс. 1–9, 2021.

[2] C. Campbell и C. Rosenyal, *Quality Assurance and Development of Course Programs*. Burcharest: Regional University Network on Governance and Management of Higher Education in South East Europe, UNESCO, 2002.

[3] CISCO, «What is Cyber Security?» 2023 г. [Онлайн]. Доступно на: https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html

[4] International Telecommunication Union (ITU), «Global Cybersecurity Index 2020: Nigeria Country Report», International Telecommunication Union, 2020.

[5] B. Kruse, T. J. Frederick, и D. K. Monticone, «Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends», *Technol. Health Care*, т. 25, вып. 1, сс. 1–10, 2017.

[6] Y. A. Makeri, «Cyber Security Issues in Nigeria and Challenges», *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, т. 7, вып. 4, сс. 315–321, 2017.

[7] T. Musa, *Cyber Security in Nigeria*. Abuja: Self-published, 2020.

[8] Nordlayer, «Cybersecurity in Education: Back to School, Back to Risks». 2023 г. [Онлайн]. Доступно на: https://nordlayer.com/blog/cybersecurity-challenges-in-education/

[9] C. Nwachukwu и P. Eze, «Ethics and Education: Towards a Reorientation of Values in Tertiary Institutions in Nigeria», *J. Afr. Educ. Res.*, т. 19, вып. 1, сс. 45–60, 2022.

[10] Nwachukwu, «Nigeria: A Failing State Teetering on the Brink», *Punch News*, май 2021.

[11] N. J. Ogunode, «Benefit of Digital Literacy for Academic Staff and Students of Tertiary Institutions in Nigeria», *Am. J. Altern. Educ.*, т. 2, вып. 2, сс. 43–53, 2025.

[12] N. J. Ogunode, A. Daniel, и A. A. Daniels, «Green Campus Initiatives in Nigerian Universities», *Int. J. Leadersh. Innov. Manag.*, т. 1, вып. 3, сс. 1–8, 2024.

[13] B. Kruse, T. J. Frederick, и D. K. Monticone, «Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends», *Technol. Health Care*, т. 25, вып. 1, сс. 12–22.

[14] E. I. Ukhami и D. Abdulsalam, «Globalisation and National Security: Perspectives on Cybersecurity Threats in Nigeria», *J. Polit. Discourse*, т. 2, вып. 1, сс. 273–286, 2024.

[15] I. A. Ajayi, A. Oluwasegun, O. Adeola, и Y. Adekunle, «Cybersecurity Governance in Nigeria: Legal Framework, Challenges, and Prospects», *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, т. 11, вып. 2, сс. 15–25.

*** Bintu Yunisa (Corresponding Author)**
Federal University Wukari, Nigeria
Email: bintunabibaty@gmail.com

Safina Abdullahi Jantullu
Shehu Shagari College of Education, Nigeria
Email: safinaabdullahijantullu@gmail.com

Offia Ogochukwu Judith
Federal University Wukari, Nigeria
Email: kenchyzd@gmail.com