E-ISSN: 2997-9439

American Journal of Education and Evaluation Studies

https://semantjournals.org/index.php/ AJEES

| Research Article

Check for updates

Cyber Security and University's Administration in Nigeria

Ahmed Idris

Nassarawa State University, Keffi, Nigeria, ahmedoguraokalla@gmail.com

Onafowope Mary Adesola, Ph.D

Department of Educational Management, St Augustine College of Education, Akoka, Lagos State, Nigeria. celineosf@yahoo.com

Oweikpodor Vera Gbaeprekumo, Ph.D

Department of Educational Management and Foundations, Delta State University, Abraka, Delta State, Nigeria. oweikpodor.vera@delsu.edu.ng/gbakumovera@gmail.com

Abstract: This study aimed to explore the benefits of integrating effective security programme into the universities' administration in Nigeria. Secondary data were used in the paper. The secondary data were collected from print and online publications. Results showed that effective protection of university' data, protection of students and staff data, stable academic programme, stable university administration, stable virtual learning programme and confidence in university integrity are benefits of integrating effective cyber security programme into the universities' administration in Nigeria. Based on the findings, the paper recommends that management of universities in Nigeria should ensure that effective cyber security programme are integrated in the university system. Adequate cyber infrastructure facilities should be provided by the government and private institutions. Staff in the management of cyber security should be constantly training on effective cyber security technique.

Keywords: Cyber security, Effective cyber security, University administration

1.0 Introduction

According to the National Policy on Education (Federal Republic of Nigerian, 2004), university education is expected to make optimum contribution to national development through the intensification and diversification of its programs for the development of high level human resources base within the context of the needs of the nation; make professional course contents to reflect Nigeria's national requirements; make all students, part of the general program of all-round improvement and to offer general study courses such as history of ideas, philosophy of knowledge and nationalism. Universities are expected to encourage and disseminate their research results to both government and industries. Universities are expected to inculcate community spirit in their students through projects and action research (Oweikpodor, Akpotu & Anho 2024). They are

expected to ensure that faculty in their professional fields have relevant industrial and specialized experience. However, the NPE states that a huge percentage of funding for university education shall be devoted to Science and Technology. The realization of university' objectives depends on effective universities' administration (Ololube, 2016).

University administration refers to the application of the universities' resources to implement the programme of the universities with the aims of realizing the objectives of the universities. University administration is the mobilization and arrangement of both human and materials resources for the achievement of the university's goals. University administration is the effective use of the resources of the university to implement the teaching programme, research programme and the community service programme of the universities. University administration is the deployment of the universities' resources to accomplish the universities' programme.

The objectives of university administration include: to implement the programme of the universities as defined; to allocate resources for the implementation of the universities programme; to ensure implementation of teaching programme, to ensure implementation of research programme; to ensure delivery of quality community services programme, to ensure effective staff development, to ensure effective student administration, to ensure smooth implementation of academic calendar and to ensure quality education (Ogunode, 2020).

Johnson in (2023) reported that the management of Babcock University has said that the school's website has been hacked by some unknown persons. The school management confirmed this development in a statement signed by the Director, Communication & Marketing of the institution, Dr Joshua Suleiman, on Wednesday. The statement read in part, "The public is hereby notified that the Babcock University management information system has been violated by suspected unscrupulous persons with intent to embarrass, deceive and defraud unsuspecting university clients and stakeholders. "The criminals had gained unauthorised, illegitimate, illicit access to some of the university's client inconsequential records from the front-end server of the university and threatened dire consequences if the university does not reach out to them, they also claim that the university's sensitive information had been compromised.

The Nigerian education sector embraced online solutions to cater for an improved record management system, e-result checker, and eLearning platform. However, this has led to increased vulnerabilities in portals of universities and other higher institutions of learning. According to Nelson, Silex secure investigators have revealed that the education sector is among the most vulnerable industries in Nigeria because it lags behind in addressing known problems. They warn that intruders could exploit known gaps to alter student records, increase incidences of identity theft, and leverage these vulnerabilities to launch massive attacks that could compromise data and even shut down portals of higher institutions (Nelson, 2025). It is based on the above that this study explore the benefits of integrating effective cyber security programme into the university administration in Nigeria.

1.2 Theoretical Approach Social Disorder/Disorganization Approach Theory

Social disorder/disorganization theory was used for this study. The Social disorder/disorganization theory was founded in early 1900s at the Chicago University and was developed by Flynn and Conrad, (1978). Holborn and Haralambos (2004) attempt to account for the effect of industrial revolution as a mitigated ecological perspective on social disorganization characterize by problem of urbanization, migration, poverty, unemployment, over-crowding given rise to various degree of crimes. The consequent of these scenarios created weaknesses in law enforcement in the social arena, due to high level of social disorder and disorganization among people. The theory however, seems to analyze the various degree of situations in Nigeria, ranging from concentration of people of questionable characters, the emerged complex environment with little accessible to scares resources, uncontrollable cross-borders migration with divergence ideologies. The theory further

attempt to explained the vulnerability of certain situation in the Nigeria, which may be a propensity in weaken the activities of law enforcement agencies, such as broken-down in the family system, either as a result of high level divorcerate, poor economic participation and backwardness in western education among others. The over whelmed scenario of Social disorder/disorganization was rather expressed via the degree of certain lapses or failure in the family functional system, which the theory laid claimed as a situation that gave rise in the formation of sub-social groups, due to the incapacitation of law enforcement agencies to offer community based services. Others are insecure national geographical/regional boundary in regulating both the influx and the activities of an individual(s) harboring criminal tendency, leading to all sort of slums in the neighborhood environment, shaping behaviors (undesirable) among members of the society.

2.0 Review of Literature

2.1 Concept of Cyber Security

Cybersecurity is an important information security principle that aims to protect computer systems, networks, and data from unauthorized access, data breaches, and other cyber threats. It involves implementing measures, protocols, and technologies to ensure the confidentiality, integrity, and availability of digital information. Cybersecurity is a categorical concept that encompasses various aspects related to protecting computer systems, networks, and information from unauthorized access, theft, damage, or disruption. It involves implementing measures to safeguard digital assets, technologies, and data, as well as mitigating risks associated with cyber threats (Khodzhanovna 2023). According to Nwachukwu (2021), cybersecurity 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.

Cyber-security is the body of guidelines or templates put in place for the protection of cyberspace. But as individuals, organizations, and even states become more dependent on cyberspace, they undoubtedly face new risks. Cybercrime can also be referred to as a series of organized crimes attacking both cyberspace and cyber security. For instance, sophisticated cyber criminals and nation states, among others, present risks to Nigeria's economy and national security. Nigeria's economic viability and national security depend on a vast array of interdependent and critical networks, services, systems, and resources known as cyberspace. Cyber-space has transformed the ways people communicate, travel, power their homes, run their economy, and obtain government services. Cybersecurity is the body of technology, processes, and practices designed to protect networks, computers, programs, and data from attacks, damage, or authorized access (Maduagwu, in Ogunode Ukozor, & Ugo-onyeka, 2025; Ugo-onyeka, Ogunode, & Ukozor, 2025). Cyber security according to Temienor, Nnorom & Oweikpodor, (2025) is the best practices that individuals or organisations can put in place to reduce the risk of an intrusion by an insider or outsider obtaining access to private information. Preventing attacks and damage to devices used by individuals and organisations, including computers, laptops, tablets, smartphones, and handhelds, as well as the internet services they use both at work and online, is the primary objective of cyber security. The objectives of school cyber security include creating a strong security posture against attacks that seek to access, alter, erase, destroy, or extort sensitive data and school or user systems, protecting student information from the public domain, and defending school confidential data from attacks. Cybersecurity is a structured approach to complete data protection (Ogunode, et al 2025; Ukhami, & Abdulsalam, 2024; Uwadia & Eti, 2018).

Cyber security are technological measures, programmes, policies and strategies designed by an individual or institutions to protect his or her data and institutional data from been accessed by an unauthorized party. Cyber security is the measure and strategies an individual and institutions designed to protects his data, networks, computer and programmes from attacks from unauthorized party (Ogunode, 2025).

2.2 Types of Threats

Schools face a range of cybersecurity threats that can jeopardise the safety of their data, disrupt educational activities, and compromise the privacy of students and staff. Here are some common threats according to Vain, (2025):

Phishing attacks

Cybercriminals often use phishing emails to trick school staff and students into providing sensitive information, such as login credentials or personal data. These emails may appear to be from legitimate sources, like school administration or trusted vendors.

Social engineering

Social engineering attacks involve manipulating individuals into divulging confidential information. Attackers may pose as IT staff, administrators or trusted individuals to trick school personnel into revealing passwords or other sensitive information.

Ransomware

Ransomware attacks involve malicious software that encrypts a school's data, making it inaccessible until a ransom is paid. Schools, which often have limited IT resources, are vulnerable to these attacks and may struggle to recover their data.

Data breaches

Schools store large amounts of personal information, including student records, staff details and financial information. A data breach can occur if unauthorised individuals gain access to this data, leading to identity theft, financial loss and privacy violations.

DDoS (Distributed Denial of Service) attacks –

DDoS attacks involve overwhelming a school's network with traffic, causing it to slow down or crash. This can disrupt online learning platforms, communications and access to school resources.

Malware –

Malware, including viruses, worms and trojans, can infect school computers and networks, leading to data loss, system outages and potential exposure of sensitive information.

Weak passwords and poor authentication practices –

Many schools face issues with weak passwords and poor authentication practices. Without strong passwords and multi-factor authentication, unauthorised users can easily gain access to school systems and data.

Unsecured Wi-Fi networks

Schools often have multiple Wi-Fi networks for students, staff and guests. If these networks are not properly secured, they can be exploited by attackers to intercept data or gain unauthorised access to school systems.

Inadequate cybersecurity training

A lack of cybersecurity awareness among staff and students can lead to accidental exposure to threats. Without proper training, individuals may fall victim to phishing, click on malicious links or use weak passwords.

Outdated software and systems

Schools often operate on tight budgets and may use outdated software and systems that lack the latest security patches, making them more vulnerable to cyber attacks.

Third-party vendor vulnerabilities

Schools often rely on third-party vendors for various services, such as learning management systems, student information systems and financial services. If these vendors have weak security measures, they can become a point of entry for cyber attacks.

Mobile device vulnerabilities

With the increasing use of mobile devices for learning, schools face the challenge of securing these devices. Unsecured mobile devices can be a target for malware, unauthorised access and data theft. These threats highlight the importance of having robust cybersecurity policies, regular training and up-to-date technology to protect school environments (Vain, 2025).

3.0 Method

This paper is a position paper. The paper depend on secondary data. This study employed a documentary research method where secondary sources of data were consulted. The method of data analysis for this study is content analysis. A documentary research method is suitable for this study because there are many of literature on the benefits of integration cyber security into the university administration in Nigeria though much of the literature is not directly linked to education (adopted from Ogunode, Ayeni, and Ogwuche 2024).

4.0 Result and Discussion of benefits of cyber security to the University System in Nigeria

According to Ogunode (2025); StrongBox (2024) & Mitigo (2024), the following are the benefits of integrating effective cyber security in the schools;

Effective protection of University's data

The school system is designed to handle and manager various data that includes financial data of the school, staff information, data on activities of the school, confidential data on bilateral agreement between international or private institutions. Deployment of cybersecurity system in the school by management can help curtain attacks on these data. Cyber security strategies employed by the school can help reduce access to these data by unauthorized party or hackers. The impact of cyber security on university administration in Nigeria goes beyond financial and operational concerns. It can also have implications for the safety and privacy of students, faculty, and staff. With the increasing use of technology in education, there is a greater risk of personal information being compromised, which can have serious consequences for individuals and the university as a whole.

Protection of students and staff data

The school keeps both students and staff vital information that are supposed to be personal data. These information are required by the schools as a criteria for admission or for employment. These information may include bank details of the staff and students bio-date. Access to these details by hackers can lead ransom collection or bullying in the part of the students. Application of cyber security programme by the schools can help the schools mitigate against hackers and to loss the data to an unauthorized party.

Stable academic programme

One of the core responsibilities of the school management is to ensure stable academic programme for both students and staff. Maintaining a stable academic programme demands that the school put everything under her control. Factor like hacking into school financial account with the financial institutions by third party will affects smooth running of the schools that will directly affects stable academic programme or the hacking of school data that have link with e-school resources and materials. This can also disrupts the academic programme of the schools but with deployment of cyber security system in the school such incidences can be minimized. Cyber security can also have a direct impact on the day-to-day administration of universities. With cyber attacks becoming more sophisticated, there is a constant risk of sensitive information being accessed or stolen. This can have serious consequences for the administration of universities, including the potential for disruption of services and damage to their reputation.

Stable school administration

The attack on school data can affects school administration because current data are needed by school administrators to plan and take decision. Data are also needed for effective allocation of school resources. The attack on these data by hackers can disrupt smooth school administration in the schools. Schools can prevent these by deploying cyber security in their schools to protect the school and student data.

Stable virtual learning programme

Most schools in Nigeria have adopted blended learning style that permitted both off-line and online learning process. The blended learning style demands the school to prepare e-learning resources to support the virtual aspect of the learning processes which include the use of e-libraries and e-platforms. The e-libraries and e-resources material or data can be hacked by unauthorized party if the necessary measure are not put in place by the school management. Stable virtual learning can be ensure in the school via deployment of cyber security system and regular update of the system.

Confidence in school integrity

School stakeholders that includes students, parents, teachers, government, non-government organizations and private institutions wants schools that are reliable and have integrity to partner with in the areas of provision of educational services. The trust, confidence and integrity of the school implies that they want schools that can be accountable in the areas of resources allocation that required presentation of data on every input of the school. The degree and extent to which theses schools can protect these data and present them at a single demands will make the stakeholder trust the school

4.1 Finding

The paper revealed that effective protection of university' data, protection of students and staff data, stable academic programme, stable university administration, stable virtual learning programme and confidence in university integrity are benefits of integrating effective cyber security programme into the universities' administration in Nigeria.

4.2 Conclusion and Recommendations

In conclusion, the impact of Cyber Security on University Administration in Nigeria is a significant and ongoing issue that requires attention and action. This study examined the benefits of integrating effective security programme into the universities' administration in Nigeria. The paper concluded that effective protection of university' data, protection of students and staff data, stable academic programme, stable university administration, stable virtual learning programme and confidence in university integrity are benefits of integrating effective cyber security

programme into the universities' administration in Nigeria. Based on the findings, the paper recommends that management of universities in Nigeria should ensure that effective cyber security programme are integrated in the university system. Adequate cyber infrastructure facilities should be provided by the government and private institutions. Staff in the management of cyber security should be constantly training on effective cyber security technique.

References

1. DOD (2025). What is cyber security education? https://www.toolbot.ai/apps/AI%20Abstracteer?desc=A%20tool%20that%20generates%20academic%20abstracts%20from%20user%20input&placeholder=Enter%20a%20topic%20for%20 0your%2 0abstract%20.
2. Editorial Team (2024). Cyber security training https://www.indeed.com/career-advice/finding-ajob/ cyber-security-training
3. Flynn, E.E., Conrad, J.P. (1978). New and Old Criminology: Arad Cover. Praeger Publishers Inc. New York
4. Federal Republic of Nigeria (FRN) (2004). *National policy of education*. Lagos, Nigeria: NERDC.
5. Howell, J. & Lind, J. (2009). Counter-Terrorism, Aid and Civil Society: Before and After the War on Terror. Basingstoke, UK: Palgrave Macmillan. ISACA, 2014).
6. Holborn, M, Haralambos, M. (2004). Sociology: Themes and Perspectives (6 Ed.) London: Harper Collins Publishers.
7. Ikuero, F. E. (2022). Preliminary Review of Cybersecurity Coordination in Nigeria. *Nigerian Journal of Technology (NIJOTECH), 41(3),pp.521-526*
8. Johnsom, H. (2023). Babcock-university-confirms-hack-of-school-website https://punchng.com/babcock-university-confirms-hack-of-school-website/
9. Khodzhanovna, S, K (2023).cybersecurity is an important information security principle. *Best journal of innovation in science, research and development,02(07), 136-169.*
10. Mitigo (2024)**.** What is cyber security training?
11. https://mitigogroup.com/cyber-security-wiki/whatis-cybersecuritytraining/#:~: text=Cybersecurity%20training%20is%20used%20to,)%2C%20networks%20and%20 cloud%20services.
12. McQuade, S. (2006). Understanding and Managing Cybercrime. Allyn & Bacon.
13. Moturi, C.A., Abdulrahim, N.R. & Orwa, D.O. (2021). "Towards adequate cybersecurity risk management in SMEs'' *International Journal of Business Continuity and Risk Management*, 11(4), pp.343- 366.
14. Nwachukwu, (2021). "Nigeria: A Failing State Teetering on the Brink." The Punch News. 19 May.
15. Nelson, N,. J. (2025). Nigeria Education Sector Vulnerable to hackers. https://comnavig.com/blog/nigeria-education-sector-vulnerable-to-hackers---by-nsikak-joseph-nelson-ceo-silex-secure-
16. Ogunode, N,. J. Ayeni, E,. O & Ogwuche, J (2024). Contribution of international organizations to the development of education in Nigeria. *Jurnal Ilmiah Pendidikan Holistik (JIPH)*, 2,(4) 345-356.

17. Ogunode, N,. J. (2025). Benefit of Digital Literacy for Academic staff and Students of Tertiary Institutions in Nigeria. *American Journal of Alternative Education* 2(2,),43-53.

18. Ogunode, N. J., Ukozor, C. U., & Ugo-onyeka, O. D. (2025). Teaching and Learning of Cyber Security Programme in Tertiary Institution in Nigeria: Problems and Way Forward. *Pioneer: Journal of Advanced Research and Scientific Progress* , *4*(1), 19–24. Retrieved from https://journals.innoscie.com/index.php/jarsp/article/view/40

19. Ololube, N. P. (2016). Education Fund Misappropriation and Mismanagement and the Provision of Quality Higher Education in Nigeria. *International Journal of Scientific Research in Education, 9*(4), 333-349

20. Oweikpodor, V. G., Akpotu, N. E. & Anho, J. E. (2024) Lecturers' attendance to Lectures in Public and Private Universities in Delta State, Nigeria. *NAEAP Journal of Studies in Educational Administration and Management*. 4: (1) 296- 306.

21. StrongBox IT, (2024). "The Role of Cybersecurity in Schools and Universities. [Online]. Available: https://www.linkedin.com/pulse/role-cybersecurity schoolsuniversitiesstrongbox-it-pvt-ltdjpdte#:~:

22. Temienor E., Nnorom, J. N., Oweikpodor, V. G., (2025) Importance of Cybersecurity Awareness Training for School Administrators and Teachers for Sustainable School System. *American Journal of Education and Evaluation Studies*. 2:(7) 267-274.

23. Ugo-onyeka, O. D., Ogunode, N. J., & Ukozor, C. U. (2025). Adequate Funding Panacea for the Development of Cyber Security Programme in Tertiary Institutions in Nigeria. *Vital Annex: International Journal of Novel Research in Advanced Sciences (2751-756X)*, *4*(1), 12–17. Retrieved from https://journals.innoscie.com/index.php/ijnras/article/view/41

24. Ukhami, E,. I. & Abdulsalam, D. (2024). Globalisation and national security: perspectives on Cybersecurity threats in Nigeria. *Journal of political discourse*, 2, 1,(2),274-286.

25. Uwadia, F. & Eti, I. F. (2018). "Cyber Security in Nigeria: Issues, Challenges and Way Forward," *International Research Journal of Advanced Engineering and Science*, 3,(2), 351-354.

26. Vain, C. (2025). Strategies for Digital Safety and Cybersecurity in Schools https://cpdonline.co.uk/knowledge-base/safeguarding/strategies-digital-safety-cybersecurity-schools