researchvision.us

Cognify: Journal of Artificial Intelligence and Cognitive Science
Vol.2 | No. 1 | 2025 pp. 12–20|ISSN: XXXX-XXXX

Cyber Security Operation and Educational Administration in Nigeria.

Okonkwo, Cecilia Okwudinma (PhD)[1]

Chinelo, E. Okonkwo [2]

[1] Department of Educational Management, Shehu Shagari University of Education Sokoto. Email: ceciliaokonkwo@gmail.com

[2] FedEx Corp Texas, USA. Email: chinelo.eokonkwo@gmail.com

Submitted: 28-Feb, 2025
Accepted: 14-Mar, 2025
Published: 29-Mar, 2025

Vol. 1, No. 1, 2025.
10.62762/JAICS.2024.000000

***Corresponding author:**
Okonkwo, Cecilia Okwudinma (PhD).[1]

Chinelo, E. Okonkwo.[2]

Department of Educational Management, Shehu Shagari University of Education Sokoto. Email: ceciliaokonkwo@gmail.com [1]

FedEx Corp Texas, USA. Email: chinelo.eokonkwo@gmail.com [2]

Copyright © 2024 by author(s) and Scientific Research Publishing Inc. This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

http://creativecommons.org/licenses/by/4.0/

Open Access

Abstract

This study focuses on cyber security operations and educational administration within the context of educational institutions in Nigeria. Through a thorough analysis of existing literature and case studies, the paper explores the concept of cyber security and cyber security threat in educational institutions. Additionally, the study examines benefits of cyber security to educational institutions in Nigeria which includes effective education-school administration, stable academic calendar, prevention of unnecessary financial costs, ensuring of data safety and privacy and assisted in building institutional trust. Based on this findings, the paper recommends that federal, states government and local government should increase the funding of educational institutions to enable administrators to institutionalize the best and cyber security operation into their institutions. Government should organize workshop for school administrators and manager of cyber security programme in the institutions to improve their knowledge and skills on effective cyber security management. Private institutions and organization should support the school administration with the provision of cyber security infrastructure facilities. School administrators should ensure school cyber are properly protected through the deployment of firewalls, antivirus software etc.

Key words: cyber security, educational administration, educational institutions

Introduction

Education is the process where an individual acquires or imparts basic knowledge to another. It is also where a person develops skills essential to daily living, learns social norms, develops judgment and reasoning, and learns how to discern right from wrong. The ultimate goal of education is to help an individual navigate life and contribute to society once they become older [1]. Education involves the transmission of knowledge, values, and skills from one generation to another, ensuring the continuity and advancement of civilizations. Education

goes beyond formal schooling, extending to informal and non-formal learning experiences. Education is the acquisition of information that include cultivation of critical thinking, creativity, problem-solving abilities, and ethical decision-making. Education empower individuals to become lifelong learners, adaptable to the challenges of a rapidly evolving world [2]. Education is a process that transfer knowledge, skills, and character traits that comes or manifests in various forms to empower the individual to be social and economic useful to himself or herself and the society. Education is an organized and planned process that leads to acquisition of knowledge from an institute of learning for personal and national development. Education is an organized learning process that facilitate acquisition of general knowledge, development of intellectual and skills for personal development as well as community development [3]. The realization of education objectives depends on effective administration and effective data administration. Nwiyi viewed educational administration as concerned with integrating the appropriate human and material resources that are made available and made effective for achieving the purposes of a program of an educational institution. Osai and Kalagbor, defined it as the process of identifying, mobilizing and utilizing scarce human and material resources relevant in education for the purpose of achieving specific educational goals efficiently and effectively [4]. Educational administration according to Okoroma, is the process that involves a careful and systematic use of methods, principles, plans and procedures necessary to achieve the educational objectives. Ogunode stated that educational administration is the application of educational resources to achieve educational goals [5]. Educational administration is the act and process of using resources in an effective and efficiency ways to attain the various objectives of educational institutions. Educational administration deals with the planning and organizing human and materials resources to realise the goals of educational institutions. Educational administration is the systematic arrangement of educational input in an operational means to achieve the set goals of educational institution [6]. Gift is of the opinion that the features of Educational Administration includes the following: (1). Educational administration doesn't refer to any single process rather different processes or aspects constitute administration. These are planning, organizing, directing, coordinating, controlling, staffing and evaluation. (2). Educational administration is a non-profit making task. (3). Educational administration is primarily a social enterprise as it is more concerned with human resources than with material resources. (4). Educational administration is more of an art than a science [7]. The reason is that human relationship prevailed here can't be maintained by any set of formulae. (5). Educational administration is similar to general administration in many ways, but it is also dissimilar to general administration in many more ways. (6). Educational administration is a complex affair. Kalagbor stated that the following activities and programmes come under the scope of educational administration at the institutional level: (a) Deciding the purposes of the

institution or school,(b) Planning for academic or curricular and cocurricular activities,(c) Preparing the time table and the time schedules for various activities,(d) Assigning duties and responsibilities to the staff members,(e) Organizing curricular and co-curricular programmes, (f) Directing and motivating the staff of the institution, (g) Coordinating by efforts of people to achieve the purpose[8]. h. Exercising control over the staff,(i) Conducting periodical reviews about the progress, achievements and failures of the institution,(j) Taking measures for staff development,(k) Maintaining order and discipline,(l) Management of materials(m) Management of finance(n) Maintaining records and registers up to date, (o)Maintaining human relationships,(p) Supervision of the work of teachers and other employees(q) Giving feedback to the teachers performing well and taking remedial measures for teachers not performing well and school data management [9]. Educational administration according to Ajayi is concerned with data collection, processing, storage, retrieval and utilization, in order to enhance the attainment of educational goals. It involves prudent management of data and a high degree of accountability. The management of data in the secondary schools like in any other organization is a cyclic process involving the principals, teachers, students, messengers and cleaners [10]. The bulk of these data are kept manually and handled by teachers and students thus making the processing, retrieval and utilization difficult [11]. Educational administration activities and programme is been done in the federal ministry of education, states ministries of education and local education authority. They handle educational planning, educational policy formulation, resources allocation and collection and storage of all education data within the country, states and local government. The need for an effective cyber security system in the operation of educational institutions in Nigeria cannot be overemphasized [12]. Cyber security according to Ogunode, Akpakwu, and Ochai, 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 [13]. Cybersecurity is a structured approach to complete data protection. Based on the above, it is import to discuss the cyber security operations and educational administration within the context of educational institutions in Nigeria.

Materials and Methods

Cyber security is one of the great human rights issues of our time. Cyber security is not only an issue for "Internet users" but for all citizens. Even someone who has never been online is directly affected when a retail company they frequent (for example, Target or Home Depot) experiences a massive consumer data breach, when their television potentially becomes a surveillance tool or when they are denied medical care because of a ransomware attack that cryptographically locks medical records and otherwise disables health care provider systems. All people and all societies are now directly affected by the security of digital systems [14]. 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 [15]. Cybersecurity includes various practices and techniques that help organizations and individuals to defend against cyberattacks. This may involve the use of firewalls, antivirus software, encryption, intrusion detection systems, and other security tools. It also includes strategies such as regular security updates, training and awareness programs, network segmentation, and incident response plans. The importance of cybersecurity has grown significantly with the increasing reliance on digital technologies and the rise in cybercrime. 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 [16]. 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: 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 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 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 [17]. 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 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, including viruses, worms and trojans, can infect school computers and networks, leading to data loss, system outages and potential exposure of sensitive information [18]. 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. 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. 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. Schools often operate on tight budgets and may use outdated software and systems that lack the latest security patches, making them more vulnerable to cyberattacks. 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 cyberattacks. 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 [19].

This paper discussed importance cyber security strategies for educational institutions in Nigeria. Among other things discussed was the concept of education, educational administration, cyber security, types of cyber threats and importance of cyber security for educational institutions in Nigeria. The study used secondary data. The content analysis method was adopted for the selection of data. The data were collected from the following sources review of published articles from reputable international journals such as CEON, Elsevier, Hindawi, JSTOR, IEEE, Learn Techlib SAGE, Nebraska and Springer amongst others.

Results and Discussion

Cyberattacks on educational institutions can have significant and far-reaching impacts that help institutions safe students, staff and institutions data. Here are some of the major benefits: effective education-school administration, stable academic calendar, prevention of unnecessary financial costs, ensuring of data safety and privacy and assisted in building institutional trust.

a) Effective education-school administration: Integration of cyber security to the educational administration and school administration in Nigeria will aid effective education-school administration. The school administrators need data for planning, policy formulation and resources allocation and these data must always be available for support this activities. Vain, observed that cyberattacks can disrupt administrative functions such as grading, attendance tracking and communication, complicating the daily operations of the school and educational institutions by attacking their cyber and collecting their data [20]. Kevin, and Schneier, etal concluded that schools and educational institutions can stopped this and protect their vital information and data from theft by using a cyber security measures and defense that can effectively protect their data from been attack easily.

b) Stable academic calendar: Adoption of effective cyber security by educational institutions can help ensure stable and effective school operation and academic activities. Vain, noted that cyberattacks, particularly ransomware attacks, can lead to the shutdown of critical IT systems, disrupting access to online classes, educational materials and digital tools necessary for learning. In severe cases, schools may need to cancel classes until systems are restored but with a sound cyber security measures in the educational institutions, this kind cyberattack can be curtain or reduce in the schools [21].

c) Prevention of unnecessary financial costs: Integration of cyber security in the educational administration and school administration in Nigeria can assists school administrators from unnecessary involvement in the payment of ransomware to third party. Vain, acknowledged that schools targeted by ransomware may face demands for payment to restore access to their systems. Even the cost of recovering from an attack alone can be substantial. Recovering from a cyberattack often requires significant investment in IT support, software upgrades and cybersecurity measures to prevent future incidents. Application of effective cyber security resilience in educational institutions can help schools and agencies from cyberattack.

d) Data safety and privacy ensured: Educational institutions with an effective cyber security strategies and technologies can prevent attack from their cyber space. This will help these educational institutions ensure students, staff and school data are kept safe and the privacy of individual data is ensured. Vain, noted that cyberattacks can lead to the theft of personal information, including student records, staff payroll data and health records. This exposure can have long-term consequences for victims, including identity theft and privacy violations but Naija Scholar concluded that such data theft can be prevented with the used of cyber security defense and protection [22].

e) Build institutional trust: The used of sound and effective cyber security defense or protection strategies can assist the educational institutions to build trust with their students, staff and stakeholders. Vain, maintained that a cyberattack can erode trust in the school's ability to protect its community, leading to concerns about the safety and security of the

school's IT infrastructure. Repeated or high-profile cyberattacks can damage the reputation of a school, leading to a loss of confidence among students, parents, staff and the broader community. Okonkwo and Ogunode, Akpakwu, and Ochai the ways institutions can build trust in their customers is by adopting the best and suitable cyber security measures in their institutions. Vain, C recommended the following strategies for effective cyber security management in educational institutions: Conducting regular risk assessment to identify vulnerabilities and threats of cyberattacks in schools is crucial for safeguarding sensitive data and ensuring the security of both students and staff. IT staff, school administrators, teachers, and possibly external cybersecurity experts should be part of this process. Define clear roles for each member, such as data collection, threat analysis and risk mitigation. All digital assets should be identified, including hardware, and the types of data being processed should be listed, for example student records, financial information and emails. Potential threats should be identified, for example phishing, malware, ransomware and DDoS attacks, and consider insider threats from staff or students, either intentional or accidental [23]. Environmental threats from natural disasters, power outages or other events that could disrupt IT systems should also be considered. Some other things to consider:

1. Assess vulnerabilities such as outdated software, unpatched systems, weak passwords, unsecured applications, unsecured Wi-Fi, unencrypted communications and lack of network segmentation. Lack of cybersecurity awareness among staff and students, poor access control and inadequate training, also need to be considered. Unsecured access to server rooms, data centres or devices can also be a risk.
2. Estimate the probability of each threat exploiting a vulnerability and assess the potential impact on the school's operations, reputation and legal standing. Combine likelihood and impact to prioritise risks. Use a risk matrix to categorise them, e.g. low, medium, and high.
3. Install firewalls, anti-malware software, encryption and multi-factor authentication (MFA). Develop policies and procedures for data handling, incident response and regular software updates. Secure physical access to sensitive areas, use surveillance systems and implement access controls. Regularly train staff and students on cybersecurity best practices.
4. Maintain a risk register that logs identified risks, their assessments and the mitigation actions taken. Generate regular reports for school leadership outlining risks and the measures taken to address them.
5. Use automated tools to continuously monitor the network for suspicious activities. Schedule periodic reviews to reassess risks and update the risk register. Conduct regular drills to ensure the effectiveness of your incident response plan.
6. Encourage feedback from staff and students to identify potential vulnerabilities that may not have been considered and stay updated on the latest cybersecurity threats and trends that could impact the school environment [24]. Regularly update security measures and training

programmes based on new risks and vulnerabilities. Establish clear goals for cybersecurity, such as protecting sensitive data, ensuring continuity of education and complying with legal standards. You should develop specific policies on:

a) Data protection

b) Access control

c) Acceptable use

d) Incident response

e) Remote learning

f) Legal compliance

School should deploy antivirus, anti-malware and firewall solutions across all devices and networks and implement encryption for sensitive data, both in transit and at rest. Ensure that all software and systems are regularly updated to protect against known vulnerabilities and separate the network into different segments, for example administrative, student and guest, to limit access to critical systems.

Implementing Technical Safeguards

a) Network Security

Implementing strong firewalls to control incoming and outgoing network traffic, and preventing unauthorised access, is important when considering network security. Deploying updated antivirus and anti-malware software on all school devices is also important.

b) Using WPA3 encryption for Wi-Fi networks and using separate student and staff networks will provide additional security. Web content filtering can block access to inappropriate or harmful websites and Intrusion Detection and Prevention Systems (IDPS) monitor network traffic for suspicious activity and can block potential threats. Virtual Private Network (VPN) ensures secure remote access for staff working from home or remote locations. Data protection in schools is a critical issue as schools handle vast amounts of personal information about students, staff and parents. Ensuring that this data is managed responsibly and securely is vital for protecting individuals' privacy and complying with legal requirements [25].

When thinking about data sharing and using third-party services, for example cloud storage and educational apps, ensure they comply with relevant data protection laws and have adequate security measures in place. Establish clear agreements outlining how data will be shared with external organisations, ensuring they understand their obligations to protect that data. There should be a plan in place for responding to data breaches. This includes notifying affected individuals and relevant authorities promptly if a breach occurs.

Establishing regular backup procedures and ensuring data recovery capabilities are critical components of digital safety for schools. Given the sensitive nature of educational data, it is essential to create a robust framework that safeguards information against loss, corruption or unauthorised access.

1. Use local servers or external hard drives to create on-site backups. Ensure that these are stored securely in a physically safe environment. Implement cloud storage solutions for off-site backups. Cloud backups provide redundancy and are less vulnerable to local disasters.
2. For critical data, set up automated daily backups. Ensure that backups happen outside of school hours to avoid disruptions. Conduct full backups weekly, capturing all data, not just the changes. Between full backups, perform incremental backups to capture only the data that has changed since the last backup.

a) Cybersecurity Awareness: Providing regular training and resources on cybersecurity best practices is essential for maintaining a secure environment in educational institutions. Develop a comprehensive curriculum covering key topics such as password security, phishing, data protection and safe internet use. There are various ways to provide training including:

Interactive workshops – host live workshops and webinars with interactive elements such as Q&A sessions and case studies [26].

E-Learning modules – provide online training modules that can be completed at the individual's convenience.

Simulations and drills – conduct phishing simulations and security drills to provide hands-on experience.

Micro-learning – offer short, focused training sessions or tips delivered via email or internal platforms.

Updates and refresher courses – regularly update training materials to reflect the latest threats and best practices. Offer refresher courses as needed.

Gamification – incorporate game elements, such as quizzes and leader boards, to make learning more engaging.

Recognition and rewards – recognise and reward individuals or teams who demonstrate strong cybersecurity practices.

Provide resources and support – create a centralised repository of resources, including guidelines, FAQs and best practice documents.

Helpdesk and support – offer access to cybersecurity experts for questions and support.

b) Creating a Cybersecurity Culture: Implement and enforce school-wide cybersecurity policies, such as acceptable use policies for technology and data protection guidelines. Start clubs or teams that focus on cybersecurity, where students can engage in projects, competitions and discussions. Encourage students to share their knowledge and experiences with their peers to foster a collaborative learning environment. Organise events like cybersecurity awareness weeks or competitions to engage students and raise awareness [27]. The paper discovered that adoption of effective cyber security strategies support effective education-school administration, stable academic calendar, prevention of unnecessary

financial costs, ensuring of data safety and privacy and assisted in building institutional trust.

Conclusion

This study focuses on cyber security operations and educational administration within the context of educational institutions in Nigeria. The paper concluded that the benefits of cyber security to educational institutions in Nigeria includes effective education-school administration, stable academic calendar, prevention of unnecessary financial costs, ensuring of data safety and privacy and assisted in building institutional trust. Based on this findings, the paper recommends that federal, states government and local government should increase the funding of educational institutions to enable administrators to institutionalize the best and cyber security operation into their institutions. Government should organize workshop for school administrators and manager of cyber security programme in the institutions to improve their knowledge and skills on effective cyber security management. Private institutions and organization should support the school administration with the provision of cyber security infrastructure facilities. School administrators should ensure school cyber are properly protected through the deployment of firewalls, antivirus software etc.

REFERENCES

[1] Ajayi, I.A (1997). Towards improving the internal efficiency of secondary schools in Ado-Ekiti Local Government area of Ekiti State. Nigerian Journal of Advanced Research, 1(1), 101-109.

[2] Benwari, N.N. &Dambo, B.I. (2014). Improving school management through transformational leadership approach and management information system. Journal of Education and Social Research, 4(6), 401-406.

[3] Eluwah, D. (2021). Cyber Awareness and Education in Nigeria: An Assessment. 10.13140/RG.2.2.23425.79202

[4] Federal Republic of Nigeria (2013). National Policy on Education 6th edition NERDC

[5] Iilsindia (2020). Cyber security education in India. https://www.iilsindia.com/blogs/cyber-security-education-in-india/

[6] Kevin, J. (2022). Importance of Cybersecurity in the education sector https://cybersecurityforme.com/importance-of-cybersecurity-in-education/

[7] Makeri, Y,. A. (2017). Cyber Security Issues in Nigeria and Challenges. International Journal of Advanced Research in Computer Science and Software Engineering, 7(4),315-321

[8] Naija Scholar (2024). Importance of cyber security education. https://disciplines.ng/importance-of-cybersecurity-

education/text=Cybersecurity%20education%20helps%20individuals%20identify,software% 20updates%20is%20also%20vital

[9] Gift, U (2018) Administration of Private Secondary Education in a Dwindling Economy in

[10] Nigeria. Journal of Resourcefulness and Distinction, 16. 1, 215

Kalagbor, L. D. (2017). Educational administration: Principles and practices in schools. Port

[11] Harcourt: Standout publishers.

Khodzhanovna, S,. K. (2023). Cybersecurity is an important information security principle. Best journal of innovation in science, research and development ,02(07),136-139.

[12] Nwachukwu, (2021). "Nigeria: A Failing State Teetering on the Brink." The Punch News. 19 May.

[13] Nwiyi, G. U. (2018). Administration of Private Secondary Education in a Dwindling

[14] Economy in Nigeria. Journal of Resourcefulness and Distinction, 16(1). 215-225

[15] Ogunode N,. J. (2020a) Challenges confronting the administration of English Language program: Secondary school context in Nigeria. Journal of Research and Innovation in Language, 2, (2), 59-6009

[16] Ogunode, N,. J. Akpakwu, F,. O & Ochai, D,. P. (2025). Cyber Security and School Management in Nigeria.

[17] Ogunode, N,. J., Solomon, A,. T & Idonigie, A (2024). The Impact of Economic Hardship on Education in Nigeria. American Journal of Management Practice, 1(6), 61-69

[18] Ogunode. N,. J. (2025). Cyber Security and Schools in Nigeria: Implication for Administrative Decision. Best Journal of Innovation in Science, Research and Development, 4(3), 146–152. Retrieved from https://www.bjisrd.com/index.php/bjisrd/article/view/3138

[19] Okonkwo, C. O. (2024). Educational Management and Artificial Intelligence in Nigerian Schools. American Journal of Technology Advancement.1(6), 1 – 9.

[20] Okonkwo, C,. O. & Okonkwo, C, E. (2024). Artificial intelligence (ai) in educational management information system (EMIS). Journal of innovation in non-formal education, 4(2),45-54

[21] Okoroma, N. S. (2016). Perspectives of educational management, planning & policy analysis. Port Harcurt: Minson publishers.

[22] Okoroma, N. S. (2016). Oil pipeline vandalization in the Niger Delta: Implications for funding education in Nigeria. Nigerian Journal of Oil and Gas Technology, 1(1), 8-18.

[23] Osai, O. J., & Kalagbor, S. B. (2017). The address on Umueri airport city project: A template for leadership in Nigeria. African Research Review, 11(3), 1-12.

[24] Schneier, D. & Bruce, C. (2016). Lessons From the Dyn DDoS Attack, Schneier on Security Blog, 8November 2016, https://www.schneier.com/blog/ archives/2016/11/lessons_ from_th_5.html

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

[26] Verma, A, Doharey, R,.K & Verma. K (2023). Education: Meaning, Definitions and Types.

[27] Worldvision (2023). Why is education important and how does it affect one's future?. https://www.worldvision.ca/stories/education/why-is-education-important World-Bank (2024) The World-bank in Nigeria. https://www.worldbank.org/en/country/nigeria/overview