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 91-99

Cyber Security Operation and Basic Education Management in Nigeria

Esther Amina Akuh
Federal University Lokoja, Nigeria

DOI : https://doi.org/10.61796/acjoure.v3i1.319

Sections Info

Article history:
Submitted: March 05, 2025
Final Revised: March 12, 2025
Accepted: March 19, 2025
Published: March 26, 2025

Keywords:
Basic education
Cyber Security
Management

ABSTRACT

Objective: *This study investigates the current state of cybersecurity operations and their integration into basic education management in Nigeria, with a focus on identifying benefits, threats, and operational challenges.* ***Method:*** *Employing a qualitative research design, the study conducts a comprehensive review and synthesis of existing literature to examine the interplay between cybersecurity and basic education systems.* ***Results:*** *The findings highlight that integrating cybersecurity into the management of basic education enhances the protection of academic records and personal data of students and staff, while also strengthening institutional integrity. However, the study identifies several challenges, including inadequate funding, limited cyber infrastructure, rapid technological changes, poor personnel training, data management complexities, staff shortages, and risks from third-party and supply chain vulnerabilities.* ***Novelty:*** *This paper contributes to the academic discourse by presenting a contextual analysis of cybersecurity issues within Nigeria's basic education sector, offering strategic recommendations such as increased funding, infrastructural support, inter-agency collaboration, and targeted capacity-building initiatives to improve cybersecurity integration and resilience in educational institutions.*

INTRODUCTION

Basic Education is the education given to children aged 0-15 years. It encompasses the Early Child Care and Development Education (0-4) and 10 years of formal schooling. Early Child Care and Development Education however is segmented into ages 0-4 years, situated in daycare or crèches, fully in the hands of the private sector and social development services, whilst ages 5-6 are within the formal education sector. The goals of Basic Education are to: a. Provide the child with diverse basic knowledge and skills for entrepreneurship, wealth generation and educational advancement; b. develop patriotic young people equipped to contribute to social development and in the performance of their civic responsibilities; c. inculcate values and raise morally upright individuals capable of independent thinking, and who appreciate the dignity of labour; d. inspire national consciousness and harmonious co-existence, irrespective of differences in endowment, religion, colour, ethnic and socio-economic background; and e. provide opportunities for the child to develop manipulative skills that will enable the child function effectively in the society within the limits of the child's capability.

The realization of Basic school objectives depends on effective management. Basic education management refer to the administration of the basic education system in which a group combines human and material resources to supervise, plan, strategise, and implement structures to execute an education system. Basic education management is the administration that oversees an education system. Educational management covers human resources, student services, financial aid, test and disability accommodations [1].

Basic education management is saddled with the functions of managing schools data for making decision and to plan the school calendar. School data includes; Schools use data from parents, students, classroom, and teacher to assess the success of the school (teacher performance, test scores, graduation rates, etc.) and to allocate resources where needed. Schools then provide data to their district, which facilitates comparative analytics across cities and regions [1].

"School districts are required to maintain comprehensive longitudinal student databases complete with information including attendance, demographics, mobility, discipline, state test scores, course enrollment, and grades earned in courses. Data systems created by districts are only useful in transforming schools when they provide meaningful data stakeholders can use to raise questions, identify issues, and make informed decisions.". District data helps administrators to understand overall demographics and academic performance [2], [3]. Data allows districts to identify the schools that need more resources versus the schools that may need different programming[4]. State and federal systems also use data to make informed choices related to district learning gaps, funding, and overall state needs. Federal and state systems create legislation, policies, and goals based on data patterns. Data received from districts and states helps lawmakers create and enforce standards and regulations to meet the academic, socio-emotional, and safety needs of all students and teachers [5], [6].

In order to manage the school data and information well, school managers globally now safe data in school cyber. Cybersecurity refers to the protection of networks, devices, and data from unauthorized or unintended access or illegal use. The same bad actors that target enterprises also look for vulnerabilities in school management. Schools need enterprise-class security measures and hardware-enabled security to help protect their students, faculty, and data from cyberattacks [7], [8].

RESEARCH METHOD

Literature Review

Concept of Cyber Security

Cyber security is a discipline that covers how to defend devices and services from electronic attacks by nefarious actors such as hackers, spammers, and cybercriminals. While some components of cyber security are designed to strike first, most of today's professionals focus more on determining the best way to defend all assets, from computers and smartphones to networks and databases, from attacks. Cyber security has been used as a catch-all term in the media to describe the process of protection against every form of cybercrime, from identity theft to international digital weapons [9]. Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyberattacks. It aims to reduce the risk of cyberattacks and protect against the unauthorised exploitation of systems, networks, and technologies [10].

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 [3]. 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." From the above, cybersecurity in this paper is a formal measures designed to protect IT systems, networks and sensitive information from attack or from unauthorized access, cyberthreats and data breaches. Cybersecurity is practical implementation of cyber security policies to ensure protection of official data within the institution [11].

Cyber security roles in educational management includes; 1) Asset security: Analyze networks, computers, routers, and wireless access points; 2) Security architecture and engineering: Standardize security policies and procedures; 3) Communication and network security: Regulate cloud storage and data transfer; 4) Identity and access management: Track user authentication and accountability; 5) Security operations: Monitor security to identify attacks; 6) Security assessment and testing: Test security policies to ensure compliance with industry standards; 7) Software development security: Create and repeatedly test code; 8) Security and risk management: Identify potential risks and implement appropriate security controls; 9) Find, test, and repair weaknesses within a institution's infrastructure.; 10) Monitor systems for malicious content; 11) Identify network breaches; 12) Install regular software updates, firewalls, and antivirus protection; 13) Strengthen areas where attacks may have occurred [9] [12].

Benefits of cybersecurity in educational institutions

The benefits of implementing and maintaining cybersecurity practices include the following: 1) School protection against cyberattacks and data breaches; 2) Protection of data and networks; 3) Prevention of unauthorized user access; 4) Improved recovery time after a breach.; 5) Protection for end users and endpoint devices; 6) Regulatory compliance; 7) School academic stability; 8) Improved confidence in the school's reputation and trust for developers, partners, customers, stakeholders and staff.

RESULTS AND DISCUSSION

Result

Functions of a Cyber Security Center:

Ideally, a Cyber Security Center should strive to ensure a secure and resilient cyber and communications infrastructure that supports national or regional security, a vibrant economy, and the health and safety of all citizens. To achieve this, a Cyber Security Center ought to: a) Serve stakeholders as a national center of excellence and expertise for cyber and telecommunications security issues. ; b) Focus on proactively coordinating the prevention and mitigation of those cyber and telecommunications threats that pose the greatest risk to the Nation; ; 3) Pursue whole-of-nation operational integration by broadening and deepening engagement with its partners through information sharing to manage threats, vulnerabilities, and incidents ; 4) Break down the technological and institutional barriers that impede collaborative information exchange, situational awareness, and understanding of threats and their impact; 5) Maintain a sustained readiness to respond immediately and effectively to all cyber and telecommunications incidents of national security; 6) Protect the privacy and constitutional rights of the citizens in the conduct of its mission [13].

Types of Cyber-threats

The following according to Shea & Gillies, are the types of cyber-threats in educational management

Malware is a form of malicious software in which any file or program can be used to harm a user's computer. Different types of malware include worms, viruses, Trojans and spyware [14].

Ransomware is a type of malware that involves an attacker locking the victim's computer system files -- typically through encryption -- and demanding a payment to decrypt and unlock them.

Social engineering is an attack that relies on human interaction. It tricks users into breaking security procedures to gain sensitive information that's typically protected.

Phishing is a form of social engineering in which fraudulent email or text messages that resemble those from reputable or known sources are sent. Often random attacks, the intent of phishing messages is to steal sensitive data, such as credit card or login information.

Spear phishing is a type of phishing that has an intended target user, organization or business.

Insider threats are security breaches or losses caused by humans -- for example, employees, contractors or customers. Insider threats can be malicious or negligent in nature.

Distributed denial-of-service (DDoS) attacks are those in which multiple systems disrupt the traffic of a targeted system, such as a server, website or other network resource. By flooding the target with messages, connection requests or packets, DDoS attacks can slow the system or crash it, preventing legitimate traffic from using it.

Advanced persistent threats (APT) is a prolonged targeted attack in which an attacker infiltrates a network and remains undetected for long periods of time. The goal of an APT is to steal data.

Man-in-the-middle (MitM)) attacks are eavesdropping attacks that involve an attacker intercepting and relaying messages between two parties who believe they're communicating with each other.

SQL injection: is a technique that attackers use to gain access to a web application database by adding a string of malicious SQL code to a database query. A SQL Q injection provides access to sensitive data and enables the attackers to execute malicious SQL statements. Other common types of attacks include botnets, drive-by-download attacks, exploit kits, malvertising, vishing, credential stuffing attacks cross site scripting attacks, keyloggers, worms and zero day exploit (Shea & Gillies, 2024).

Benefits of Integration of Cyber Security to Management of Basic Education in Nigeria

The benefits of integrating cyber security to management of basic education in Nigeria includes; protection of academic records, students and staff data and promote the integrity of the institutions.

Protection of academic records

Cyber security operation in the management of basic education in Nigeria will help to protection academic records with the institutions. With well cyber security measure and strategies, attacks will not be able to access these data and use them for illegal dealings. Schools need enterprise-class security measures and hardware-enabled security to help protect their students, faculty, and data from cyberattacks.

Students and staff data

The used of cyber resilience and cyber security measures in the management of basic education in has assisted in the protection of student and staff information from been attacked by third party. The integration of cyber security in the management of basic education in Nigeria has helped to an extent in the protection of sensitive personnel details from threats. Cyber security aids protection of school data from threats (Ding, 2000).

Promote the integrity of the institutions

The adoption of cyber security in the management of basic education have boosted the confidence of staff, students and parents on the integrity of the institutions in Nigeria. Parents and students have confident that with the adoption of good cyber security system in management of basic education, their data are protected from threats.

Discussion

Cyber Security Challenges in Management of Basic Educational

The challenges facing cyber security integration to management of basic education includes; inadequate funding, shortage of cyber infrastructure facilities, technology advancement, problem of large data, poor training on cybersecurity, personnel shortage and supply chain attacks and third-party risks.

Inadequate funding

Inadequate funding is a major problem militating against the development of cyber security development in the integration of cyber security and management of basic education in Nigeria. The budgetary allocation to education in Nigeria is not adequate to implement cyber security programme fully in the educational institutions.

Shortage of cyber infrastructure facilities

Another problem hindering the full integration of cyber security to the management of basic education is the problem of inadequate cyber infrastructure facilities. Many educational institutions in Nigeria do not have adequate cyber security infrastructure facilities in their respective schools. This shortage is due to poor funding of the educational sector.

Technology advancement

Shea, S & Gillies, observed that one of the most problematic elements of cybersecurity is the evolving nature of security risks. As new technologies emerge -- and as technology is used in new or different ways -- new attack avenues are developed [14]. Keeping up with these frequent changes and advances in attacks, as well as updating practices to protect against them, can be challenging. Issues include ensuring all elements of cybersecurity are continually updated to protect against potential vulnerabilities. This can be especially difficult for smaller organizations that don't have adequate staff or in-house resources.

Problem of large data

Shea & Gillies, noted that organizations can gather a lot of potential data on the people who use their services [14]. With more data being collected comes the potential for a cybercriminal to steal personally identifiable information (PII). For example, an organization that stores PII in the cloud could be subject to a ransomware attack. Cyber security measures help school to protect students and staff data [15].

Poor training on Cybersecurity

Shea & Gillies, (2024) maintained that cybersecurity programs should also address end-user education. Employees can accidentally bring threats and vulnerabilities into the workplace on their laptops or mobile devices. Likewise, they might act imprudently -- for example, clicking links or downloading attachments from phishing emails. Regular security awareness training can help employees do their part in keeping their company safe from cyber-threats.

Personnel Shortage

Another cybersecurity challenge according to Shea & Gillies, is a shortage of qualified cybersecurity personnel. As the amount of data collected and used by businesses grows, the need for cybersecurity staff to analyze, manage and respond to incidents also increases [14]. In 2023, cybersecurity association ISC2 estimated the workplace gap between needed cybersecurity jobs and security professionals at 4 million, a 12.6% increase over 2022.

Supply chain attacks and third-party risks

Shea & Gillies, opined that organizations can do their best to maintain security, but if the partners, suppliers and third-party vendors that access their networks don't act securely, all that effort is for naught. Software- and hardware-based supply chain attacks are becoming increasingly difficult security challenges [14]. Organizations must address third part risk in supply chain and reduce software supply issues, for example, by using software bills of materials.

Cybersecurity best Practices for Educational Management

To minimize the chance of a cyberattack, it's important to implement and follow a set of best practices that includes the following:

Keep software up to date. Be sure to keep all software, including antivirus software, up to date. This ensures attackers can't take advantage of known vulnerabilities that software companies have already patched.

Change default usernames and passwords. Malicious actors might be able to easily guess default usernames and passwords on factory preset devices to gain access to a network.

Use strong passwords. Employees should select passwords that use a combination of letters, numbers and symbols that will be difficult to hack using a brute force attack or guessing. Employees should also change their passwords often.

Use multifactor authentication (MFA). MFA requires at least two identity components to gain access, which minimizes the chances of a malicious actor gaining access to a device or system.

Train employees on proper security awareness. This helps employees properly understand how seemingly harmless actions could leave a system vulnerable to attack. This should also include training on how to spot suspicious emails to avoid phishing attacks.

Implement an identity and access management system (IAM). IAM defines the roles and access privileges for each user in an organization, as well as the conditions under which they can access certain data.

Implement an attack surface management system. This process encompasses the continuous discovery, inventory, classification and monitoring of an organization's IT infrastructure. It ensures security covers all potentially exposed IT assets accessible from within an organization.

Use a firewall. Firewalls restrict unnecessary outbound traffic, which helps prevent access to potentially malicious content.

Implement a disaster recovery process. In the event of a successful cyberattack, disaster recovery plans helps an organization maintain operations and restore mission-critical data [14].

CONCLUSION

Fundamental Finding : The research identifies critical challenges such as inadequate funding, limited cyber infrastructure, insufficient personnel training, and increasing third-party risks, which hinder the full realization of cybersecurity in basic education. **Implication :** These findings underscore the urgent need for a multi-stakeholder approach involving government agencies, educational institutions, and industry partners to promote investment in cybersecurity capacity building, infrastructure, and policy frameworks. **Limitation :** The study is limited by its reliance on secondary data and literature review, which may not capture recent institutional-level developments or region-specific variations in cybersecurity practices. **Future Research :** Further empirical investigations are recommended to explore the practical implementation of cybersecurity measures in Nigerian schools and to assess the effectiveness of existing frameworks in diverse educational contexts.

REFERENCES

[1] N. J. Ogunode, A. Abdulrazak, and J. A. Abubakar, "Digitalization of Educational Institutions in Nigeria: Benefits, Problems and Solutions," *World Semant. J. Philos. Linguist.*, vol. 2023, pp. 13–21, 2023.

[2] E. I. Ukhami and D. Abdulsalam, "Globalisation and National Security: Perspectives on Cybersecurity Threats in Nigeria," *J. Polit. Discourse*, vol. 2, no. 1, pp. 273–286, 2024.

[3] D. Schneier and C. Bruce, "Lessons From the Dyn DDoS Attack," *Schneier on Security Blog*. Nov. 2016.

[4] ITU, "Global Cybersecurity Index 2020: Nigeria Country Report." 2020.

[5] Learninga-z, "Resources." 2020.

[6] N. J. Ogunode, V. O. Ayoko, and V. Orifah, "Digitalization of Post-Basic Education and Career Development (PBECD) in Nigeria: Problems and Way Forward," *Eur. Multidiscip. J. Mod. Sci.*, vol. 19, pp. 32–40, 2023.

[7] S. S. Oyelere, D. I. Sajoh, Y. M. Malgwi, and L. S. Oyelere, "Cybersecurity Issues on Web-Based Systems in Nigeria: M-Learning Case Study," in *2015 International Conference on Cyberspace, CYBER-Abuja*, Institute of Electrical and Electronics Engineers, 2015, pp. 259–264.

[8] C. M. Ding, "Access to Digital Information: Some Breakthrough and Obstacles," *J. Librariansh. Inf. Sci.*, vol. 32, no. 1, 2000.

[9] K. Kelly, "What is Cyber Security | Types, Importance and Threats." 2025.

[10] ITgovernance, "What is Cyber Security?" 2024.

[11] T. O. Adeyemi, "Principals' leadership styles and teachers' job performance in senior secondary schools in Ondo State, Nigeria," *Int. J. Educ. Adm. Policy Stud.*, vol. 2, no. 6, pp. 83–91, 2010.

[12] Y. A. Makeri, "Cyber Security Issues in Nigeria and Challenges," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 7, no. 4, pp. 315–321, 2017.

[13] E. E. Akpan, "A Critical Analysis of Cyber Security and Resilience in Nigeria," *World Atlas J. Libr. Inf. Sci.*, vol. 5, no. 1, pp. 10–22.

[14] S. Shea and A. S. Gillies, "What is Cyber Security?" 2024.

[15] N. J. Ogunode, F. O. Akpakwu, and D. P. Ochai, "Cyber Security and School Management in Nigeria," 2025.

*** Esther Amina Akuh (Corresponding Author)**
Federal University Lokoja, Nigeria
Email: estheraminaakuhg2@gmail.com