International Journal of Business, Law and Political Science
Homepage : https://e-journal.antispublisher.id/index.php/IJBLPS
Email : admin@antispublisher.com

e-ISSN : 3032-1298
IJBLPS, Vol. 2, No. 5, May 2025
Page 181-191
© 2025 IJBLPS :
International Journal of Business, Law and Political Science

Cyber Security and School Management in Nigeria

Niyi Jacob Ogunode[1], Florence Onyemowo Akpakwu[2], Donatus Peter Ochai[3]
[1,2,3]Independent Research, Nigeria

DOI : https://doi.org/10.61796/ijblps.v2i5.317

Sections Info

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

Keywords:
Cyber security
School management

ABSTRACT

Objective: *This study examines the significance of effective cybersecurity management in Nigerian schools and its implications for data protection, legal compliance, and educational stability.* ***Method:*** *A qualitative analysis was conducted, reviewing relevant policies, existing cybersecurity frameworks, and their application within the Nigerian education sector.* ***Results:*** *The findings indicate that adopting cybersecurity measures enhances the protection of sensitive school data, ensures compliance with the Child Rights Act and record-keeping regulations, fosters a stable learning environment, safeguards intellectual property, supports remote and virtual learning, and facilitates informed decision-making in school management.* ***Novelty:*** *This study highlights the critical role of cybersecurity in maintaining the integrity and security of educational institutions in Nigeria, emphasizing the necessity for structured policies and training programs. It underscores the need for federal, state, and local education authorities to implement comprehensive cybersecurity strategies and provide professional development for educators and school administrators. Additionally, it advocates for stronger stakeholder engagement in cybersecurity initiatives to ensure effective implementation and sustainability.*

INTRODUCTION

In order to enable an individual to be socially and economically beneficial to both themselves and society, education is a process that transfers knowledge, skills, and character qualities that can take many different forms. Education is a planned, structured process that results in information acquisition from a learning institution for both individual and societal advancement. Education is a structured process of learning that promotes the development of general knowledge, intellectual capacity, and skills for both individual and collective growth [1]. In order to maintain the continuity and progress of civilisations, education entails passing along knowledge, values, and skills from one generation to the next. Education includes both informal and non-formal learning activities in addition to regular schooling. Education is the study of knowledge combined with the development of critical thinking, creativity, problem-solving skills, and moral judgement. Through education, people can develop into lifelong learners who can adapt to the needs of a rapidly changing world [2]. Learning to better understand a variety of subjects that can be applied to daily tasks is the process of education. Books are not the only source of education; activities outside of the classroom can also provide valuable insights [3]. Education is the process by which a person acquires or imparts basic knowledge to another person. It is also where people learn social norms, strengthen their judgement and reasoning abilities, learn to distinguish between good and wrong, and pick up skills that are essential for day-to-day functioning. Education's ultimate goal is to help people navigate life and make contributions to society as they age [4]. Education is one instrument for affecting the growth of a country. Education may be defined as the production and distribution of knowledge about people's lifestyles or cultures in order to maintain and support the social structure that will be able to guarantee social order and social transformations in the community [5]. The aforementioned states that education is the process of teaching someone economic, social, leadership, and ICT skills to enable them integrate into society on both a social and economic level. Education is the systematic teaching of knowledge, skills, and character in a controlled environment for the development of the individual and the community. The National Education Policy [6] offers a road map for attempting to accomplish the nation's objectives. According to the Second National Development Plan [5], this country's five primary objectives are to produce a free and democratic society, a just and egalitarian society that is united as a strong and self-reliant nation, a great and dynamic economy, and a land of bright and full of opportunities for all citizens. The accomplishment of educational objectives depends on efficient school administration. Education management is concerned with the efficient and effective organisation and management of school resources in order to accomplish school objectives. Under the condition that current data is available, school management is responsible for allocating resources for planning and decision-making. School officials and students now prioritise cybersecurity in the classroom due to the rise in digital breaches. While students encounter privacy invasion, financial fraud, and identity theft, cybercrimes can cause financial loss, lawsuits, operational disruptions, student data breaches, and a decline in trust for educational institutions. Examining the benefits for Nigerian school administrators makes discussing and researching the various cyber security school management strategies essential.

Literature Review

Concept of School Management

The internal administration of the educational system is known as school management, and it involves a team of people and material resources working together to oversee, monitor, inspect, and put into place the structures needed to carry out the policies and programs of the school. The internal administration of the school structure for better resource allocation performance is referred to as school management. Its overarching objective is to provide and preserve conditions in educational institutions and school administration that effectively and efficiently support, encourage, and sustain teaching and learning within the school system. The term "school management" refers to the internal operations of the school with the goal of carrying out the curriculum by allocating resources in a way that is both effective and efficient. It considers every facet of the school, including its structure, rules, laws, and people and material resources. The goals of school administration are as follows:

1. It facilitates the efficient and successful operation of the organisation.
2. It establishes the school's policies, guidelines, and rules.
3. It establishes the organization's framework.
4. It specifies the roles, responsibilities, authority, and power of the various positions inside the company.

5. It offers active supervision and competent professional leadership.
6. It organises the institution's many activities.
7. It establishes favourable circumstances for study and experimentation.
8. It strives for efficient communication to sustain improved human relations and working circumstances.
9. It settles the different disputes that occur inside the organisation.
10. It supports the institution's socially responsible operations and guarantees the community's socioemotional growth. Plant management, school supervision, school finances, school-community relations, curriculum development, academic calendar planning, staff-student management, extracurricular management, sport management, and school data management, including cyber security, are all included in the broad category of school management. Effective student, staff, and school data protection, storage, and distribution to the relevant department for planning and decision-making are among the duties borne by school managers. The accomplishment of the school's goals depends on an efficient cyber security program.

Concept of Cybersecurity

Cybersecurity is the practice of protecting systems, networks, and programs from internet threats. Usually, the goal of these breaches is to interfere with normal business activities, use ransomware to demand money from clients, or access, change, or remove private information [6]. Cybersecurity is the process of protecting data, software, hardware, and other internet-connected systems from cyberattacks. It is used by both individuals and companies to prevent unauthorised access to electronic systems, such as data centres [7]. Cybersecurity, according to Nwachukwu, is a collection of policies, security ideas, tools, security safeguards, risk management techniques, guidelines, activities, best practices, training, assurance, and technology that are used to secure the cyber environment, organisation, and user assets. Examples of organisational and user assets include connected computing devices, personnel, programs, infrastructure, services, telecommunications systems, and all data stored and/or transported in the cyber environment. Protecting users' assets and the organization's security properties against relevant security threats in the online environment is the aim of cyber security [8]. According to Kruse, Frederick, Jacobson, and Monticone [9], cyber security is a set of practices and protocols for defending computers, networks, databases, and applications against intrusions, unauthorised access, alteration, or destruction. Furthermore, it could be crucial for the development of information technology and Internet services. The International Telecommunications Union [ITU] defines cybersecurity 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 organisation and user's assets." Examples of an organization's and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and all data stored and/or transported in the cyber environment. The ITU states that the three primary security objectives are secrecy, integrity (which may include authenticity and non-repudiation), and availability. While these three objectives serve as the cornerstone of a secure network, achieving them requires the coordination of several departments, such as robust systems engineering and configuration management, an effective cyber security or information assurance strategy, and comprehensive employee training. Protecting users' assets and the organization's security properties from relevant security risks in the cyber environment, which includes the internet, is the goal of cybersecurity [6]. Cybersecurity can also be defined as the set of methods, techniques, and instruments designed to protect computers, networks, software, and data from damage, unlawful access, and intrusion [10]. As stated above, in this text, cyber security refers to intentional plans, programs, and technologically focused policies and techniques designed to protect institutional data, personal data, programs, and resources against damage and assault by unauthorised parties. Cyber security refers to 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. One advantage of cyber security in educational institutions is that it protects businesses and school administration from data breaches and cyberattacks.

1. Preventing assaults on school networks and data.
2. Preventing unwanted users from accessing school websites.
3. After a compromise, effective cyber protection speeds up recovery.
4. Defence against attacks on school endpoint devices and end users.
5. It helps schools secure student data and ensure that it complies with educational rules and regulations.
6. Stable academic work is supported by appropriate cyber security measures, which safeguard digital learning resources that are essential to long-term school learning.
7. Parents, students, partners, and other education stakeholders are more confident in the school's reputation and trust when there is effective cyber security in place.

Types of Cybersecurity Threats

Cybersecurity threats can come in various forms, and the following are the most common types of cybersecurity threats according to Cypfer [11]:

1. Malware

Malware is malicious software designed to harm or gain unauthorized access to a computer system. It includes viruses, worms, and Trojans.

2. Phishing

Phishing is a type of social engineering attack where cybercriminals trick people into giving away sensitive information such as usernames, passwords, and credit card details.

3. Ransomware

Ransomware is a type of malware that encrypts data on a victim's computer and demands payment in exchange for the decryption key.

4. Denial of Service (DoS) Attacks

A DoS attack is an attempt to overwhelm a network or website with traffic, causing it to crash or become unavailable.

5. Insider Threats

Insider threats occur when an employee or contractor with authorized access to sensitive data or systems intentionally or unintentionally causes harm to an organization.

6. Advanced Persistent Threats (APTs)

APTs are complex, targeted attacks designed to gain unauthorized access to a network or system and remain undetected for an extended period.

Types of cybersecurity

The six types of cyber security according to Cypfer includes [12];

1. Network Security

The process of protecting a computer network from intrusions or attacks is known as network security. It involves using virtual private networks (VPNs), intrusion detection and prevention systems, and firewalls. Protecting a network's infrastructure, which includes servers, routers, switches, and other network devices, is the main objective of network security. Important aspects of network security include:

a. Network monitoring and management tools.
b. Access control and authentication systems.
c. Data encryption and decryption methods.
d. Firewall technology.
e. Regular security audits.

2. Application Security

The steps done to protect software programs against cyberattacks are referred to as application security. It involves evaluating the code, spotting security holes, and making sure the program is error-free. From planning to deployment, application security can be applied at different phases of the software development life cycle. Important aspects of application security include:

Code review and vulnerability scanning
Use of secure coding practices
Implementation of secure authentication and authorization mechanisms
Regular security testing and update

3. Information Security

Protecting digital data, including that which is kept in files, databases, and other repositories, is known as information security. Information security shields data against unwanted access, disclosure, alteration, and destruction, ensuring its availability, confidentiality, and integrity. It incorporates a number of security features, including backups, encryption, and access control. Important aspects of information security include:

a. Using two-factor authentication, biometric verification, or passwords as access control methods.
b. Sensitive data encryption both in transit and at rest.
c. Maintaining regular backups of important data.
d. Putting business continuity and disaster recovery plans into action.
e. System and network activity monitoring and logging.

4. Cloud Security

Protecting data and systems housed on cloud platforms like Google Cloud, Microsoft Azure, and Amazon Web Services (AWS) is known as cloud security. To protect both the data stored in the cloud and the cloud infrastructure itself, cloud security consists of a mix of administrative and technical safeguards. Important aspects of cloud security include:

a. Utilising virtual private networks and secure cloud configurations.
b. Putting identity and access management controls into place.
c. Data encryption both in transit and at rest.
d. Frequent compliance inspections and security audits.

5. Internet of Things (IoT) Security

The network of interconnected gadgets, including wearables, smart homes, and smartphones, is referred to as the Internet of Things (IoT). IoT security entails protecting both the network that links the devices and the devices themselves. The risk of cyberattacks rises with the quantity of IoT devices. Important aspects of IoT security include:

a. Putting secure communication techniques into practice.
b. Frequent patches and software upgrades.
c. Employing robust access control and authentication systems.
d. Data integrity checks and encryption.
e. Frequent penetration tests and vulnerability assessments.

6. Identity and Access Management (IAM)

Managing user identities and regulating resource access inside a company is known as identity and access management, or IAM. IAM incorporates a number of security features, including access control, authorisation, and user authentication. Important aspects of IAM:

a. Making use of robust authentication techniques like two-factor authentication or biometric verification.
b. Role-based access control implementation.
c. Frequent compliance inspections and security audits.
d. Putting password policies into place and changing them frequently.

RESEARCH METHOD

This paper takes a stance. Secondary data was used in the paper. Print and internet publications provided the secondary data. The literature used in the paper was chosen using content analysis. International publications including CEON, Elsevier, Hindawi, JSTOR, IEEE, Learn Techlib SAGE, Nebraska, and Springer are typically included as references for the literature. This essay takes a stance. Secondary data was used in the paper. Print and internet publications provided the secondary data. The literature used in the paper was chosen using content analysis. International publications including CEON, Elsevier, Hindawi, JSTOR, IEEE, Learn Techlib SAGE, Nebraska, and Springer are typically among the literature's sources.

RESULTS AND DISCUSSION

Data Analysis on Benefits of Effective Cybersecurity Measures in Schools in Nigeria

Adopting cyber security strategies in Nigerian schools will improve the protection of sensitive school data, help schools comply with the Child Act and the Record Keeping Act, create a stable learning environment, protect intellectual property, facilitate remote and virtual learning, and guarantee that school data is available for planning and decision-making. These are just a few advantages of implementing effective cyber security measures in school management.

Protection of Sensitive School Data

Schools in Nigeria would be able to safeguard critical school data that is necessary for management consumption alone if they implement an efficient cyber security plan. Government policies and programs for schools have noted that educational institutions store personal information of students, faculty, and staff, including names, addresses, academic records, and financial details. These data include financial records, student data results, and student and staff information. This data is shielded from theft and unauthorised access by cybersecurity measures [13].

Compliance with Child-Act law and record keeping Act of Nigeria

Nigeria's educational law requires educational institutions to securely maintain and efficiently manage student records. Efficient cyber security measures in Nigerian schools would guarantee that student records are maintained appropriately without exposing them and aid to comply with these requirements. StrongBox IT pointed out that regulations such as the Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA) in the US establish standards that educational institutions must follow [13]. These regulatory frameworks emphasise how crucial it is to protect the data of minors, requiring schools to implement safeguards and imposing penalties for noncompliance.

Stable Learning

A stable and secure learning environment will be maintained in Nigerian schools with the support of effective cyber security measures. A school's website where students can access digital materials for learning can be prevented from going down with the use of effective cyber security measures. When schools have the capacity to stop ransomware cyberattacks, they can effectively avoid and manage them. Nordlayer noted that schools have been particularly hard struck by ransomware, which is malicious software that encrypts files and demands payment to unlock them. Regaining access to their system often costs prestigious colleges hundreds of thousands of dollars. Cyberattacks utilising ransomware can interfere with education by preventing access to digital resources, resulting in downtime, and impeding learning [14].

Protection of Intellectual Property

Protecting intellectual property and school cyberspace will be made easier with the implementation of effective cyber security measures in Nigerian educational institutions. Research conducted by schools, particularly those at higher education institutions, fosters creativity and the creation of novel concepts. Through an efficient cyber security strategy and procedures, school administration can easily preserve these research findings and results, which are in the form of fresh knowledge about services or goods that belong to individuals in the schools or even own by the institutions. Universities and research facilities, according to StrongBox IT, are centres of creative thinking and exclusive research. Cybersecurity protects intellectual property against theft or cyberespionage [13].

Support Remote Learning and Virtual learning

Nigerian educational institutions are embracing distance learning. According to Ogunode and Ukozor, the Nigerian Federal Government created the Core Curriculum and Minimum Academic Standards (CCMAS), a new curriculum for universities. The academic year 2023–2024 marks the start of the CCMAS's implementation. The CCMAS was designed using a blended and hybrid learning approach. This is because, in the event of an emergency such as COVID-19, institutions ought to have the option to transition to a different model. Musa pointed out that several Nigerian educational institutions have embraced various online learning models that work well for their settings [15]. The kind of learning model known as remote learning occurs when students, teachers, and information sources are not physically present in a conventional classroom setting. Technology or digital tools like discussion boards, video conferencing, and online tests are frequently used in the teaching and learning process. To prevent external adversaries from disrupting or attacking these digital resources, Nigerian schools must implement cyber security measures. According to StrongBox IT, strong cybersecurity procedures are essential to safeguarding the integrity of communication tools and remote learning platforms as online and hybrid learning environments grow in popularity.

Availability of School Data

Good cyber security management in Nigerian schools would guarantee that school data is available for planning, allocating resources, and making decisions. Due to inadequate cyberspace management, many educational institutions leave their kids, employees, and school data vulnerable to attackers that exploit the weak system. According to studies, numerous schools have lost critical data to cyberattacks, which has impacted management since they are unable to obtain up-to-date information for making decisions and making plans for the schools. There have been numerous complaints from parents and students about their private information being made public. According to Ogunode et al. (2023), Nigerian schools can guarantee the protection of school data for efficient budget and school planning by implementing strong cybersecurity policies and methods.

Measures to Adopt for effective Cyber Security Management in Schools

To guarantee efficient cyber security management in their own schools, Nigerian schools might implement a variety of cyber security tactics. What Cypfer proposed was:

Use of Antivirus and Anti-malware Software

Essential tools that can help shield your computer against ransomware, spyware, and viruses include antivirus and anti-malware software. To find any possible risks, make sure your antivirus and anti-malware software is up to date and perform scans on a regular basis.

Regular Software Updates

Security patches that address known vulnerabilities are frequently included in software updates. Make that the school updates its operating system, web browsers, and other software programs on a regular basis.

Strong Passwords and Multi-Factor Authentication

Multi-factor authentication and strong passwords can help keep your accounts safe from unwanted access. Make sure that students' and the school's passwords contain a mix of capital and lowercase characters, digits, and symbols. Enable multi-factor authentication on all accounts that support it as well.

Education and Awareness:

Both individuals (students) and organisations (schools) can benefit from cybersecurity education and awareness by being able to recognise possible cyberthreats and take the appropriate safety measures. To keep abreast of the most recent security dangers and best practices, make sure educators and students receive frequent cybersecurity training.

Also, CISCO recommended the following measures;

Regular software and operating system updates

Patching vulnerabilities and improving security measures against possible threats are made easier with regular operating system and software updates.

Using strong and unique passwords

Since weak or stolen passwords are frequently used by cybercriminals, creating strong and one-of-a-kind passwords for every online account helps improve cybersecurity.

Implementing multi-factor authentication (MFA)

By requiring several pieces of identity prior to account access, multi-factor authentication lowers the possibility of unwanted access. MFA is a feature of Cisco Duo that can interface with both bespoke apps and the majority of popular apps. Additionally, the optimum cybersecurity strategy should have many layers of defence across any potential attack surface or access point, according to the Tech-target Editorial Team. This provides a layer of protection for linked networks, hardware, software, and data. Every employee at a company who has access to any of these endpoints should also receive training on the appropriate security and compliance procedures. As an additional line of defence against attacks, educational institutions also employ tools like unified threat management systems. Potential hazards can be identified, isolated, and fixed by these technologies, which can also alert users when further action is required.

Findings

The implementation of cyber security measures in Nigerian schools is expected to enhance the following: learning stability, intellectual property protection, adherence to the Child Act and the Record Keeping Act of Nigeria, safeguarding sensitive school data, facilitating remote and virtual learning, and making school data available for planning and decision-making. The use of antivirus and anti-malware software, regular software updates, the use of strong passwords and multi-factor authentication, staff and student education and awareness, and the employment of qualified cyber security officers are a few tactics Nigerian schools can employ to manage cyber security.

CONCLUSION

Fundamental Finding : This study underscores the critical role of cybersecurity in Nigerian school management, highlighting its importance in protecting student data, ensuring compliance with legal frameworks, fostering a secure learning environment, safeguarding intellectual property, and supporting digital education initiatives. **Implication :** The findings suggest that a structured cybersecurity framework is essential for educational institutions to mitigate cyber threats, maintain operational efficiency, and enhance trust in digital learning systems. Government agencies, school administrators, and stakeholders must collaborate to implement and sustain effective cybersecurity policies. **Limitation :** This study primarily relies on qualitative analysis and does not incorporate empirical data or case studies from Nigerian schools, which may limit the generalizability of the findings. **Future Research :** Further research should explore the effectiveness of existing cybersecurity policies in Nigerian schools, assess the awareness and preparedness of educators in managing cyber threats, and examine the impact of cybersecurity investments on educational outcomes through quantitative and comparative analysis.

REFERENCES

[1] N. J. Ogunode, T. S. Ajape, and A. Idonigie, “The Impact of Economic Hardship on Education in Nigeria,” *Am. J. Manag. Pract.*, vol. 1, no. 6, pp. 61–69, 2024.

[2] A. Verma, R. K. Doharey, and K. Verma, *Education: Meaning, Definitions and Types*. 2023.

[3] M. A. Abu Al-Majd, “Research business incubators and the development of the university’s competitive capacity,” *Arab J. Stud. Educ. Psychol. ASEP*, vol. 66, pp. 305–331, 2015.

[4] Worldvision, “Why is education important and how does it affect one’s future?” 2023. [Online]. Available: https://www.worldvision.ca/stories/education/why-is-education-important

[5] National Open University of Nigeria (NOUN), *Issues and Problems in Higher Education in Nigeria*. Lagos, Nigeria, 2012.

[6] CISCO, "What is Cyber Security?" 2023. [Online]. Available: https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html

[7] Teacherscript, "School Management." 2022. [Online]. Available: https://www.teacherscript.com/2022/05/school-management-meaning-concepts.html

[8] Nwachukwu, "Nigeria: A Failing State Teetering on the Brink," *Punch News*, May 2021.

[9] B. Kruse, T. J. Frederick, and D. K. Monticone, "Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends," *Technol. Health Care*, vol. 25, no. 1, pp. 1–10, 2017.

[10] A. O. Hassan, S. K. Ewuga, and A. A. Abdul, "Cybersecurity in banking: A global perspective with a focus on Nigerian practices," *Comput. Sci. Secur.*, 2024, [Online]. Available: https://www.researchgate.net/publication/379038844_CYBERSECURITY_IN_BANKING_A_GLOBAL_PERSPECTIVE_WITH_A_FOCUS_ON_NIGERIAN_PRACTICES

[11] Cypfer, "What are the Six Types of Cyber Security?" 2024. [Online]. Available: https://cypfer.com/what-are-the-6-types-of-cyber-security/#:~:text=The%206%20types%20of%20cybersecurity%20measures%20discussed%20in%20this%20article,and%20individuals%20from%20cyber%20attacks.

[12] Cypfer, "What are the six types of cyber security?" 2024. [Online]. Available: https://cypfer.com/what-are-the-6-types-of-cyber-security/#:~:text=The%206%20types%20of%20cybersecurity%20measures%20discussed%20in%20this%20article,and%20individuals%20from%20cyber%20attacks.

[13] StrongBox IT, "The Role of Cybersecurity in Schools and Universities." 2024. [Online]. Available: https://www.linkedin.com/pulse/role-cybersecurity-schools-universities-strongbox-it-pvt-ltd-jpdte#:~:text=Protection%20of%20Sensitive%20Data%3A%20Educational,from%20theft%20or%20unauthorised%20access.

[14] Nordlayer, "Cybersecurity in Education: Back to School, Back to Risks." 2023. [Online]. Available: https://nordlayer.com/blog/cybersecurity-challenges-in-education/

[15] E. G. Musau, "Supply Chain Management and Organizational Performance Among Kenyan Textile Firms: A Moderated Mediation Model of Government Support and Environmental Uncertainty," *Int. J. Manag. Value Supply Chains*, vol. 11, no. 3, pp. 17–28, 2020.

***Niyi Jacob Ogunode (Corresponding Author)**
Independent research, Nigeria
Email: niyijacobogunode@gmail.com

Florence Onyemowo Akpakwu
Independent research, Nigeria
Email: akpakwufloxy@gmail.com

Donatus Peter Ochai
Independent research, Nigeria
Email: donoch2001@yahoo.com