

INTEGRATING CYBER SECURITY INTO EDUCATIONAL MANAGEMENT IN NIGERIA: A REVIEW PAPER

By

Dr. Emmanuel Ukata, CMF

Augustine Institute of Philosophy

&

Cynthia Nneka Oliagba, DMMM

Department of Educational Management, University of Abuja, Abuja

Abstract

This study aims to examine the effects of integrating cyber-security in educational management in Nigeria. The study utilizes a quantitative research design, incorporating systematic review method in data collection and analysis techniques. The results of this study provide insight into the import of integrating cybersecurity in educational institutions and the potential impact of implementing cyber-security in educational management. This research informs educational leaders on the importance of taking a proactive approach to cybersecurity and provide recommendations for integrating cybersecurity into educational management practices. Furthermore, this study contributes to the existing literature on cybersecurity in educational settings and assist in identifying potential gaps in current practices. Ultimately, the findings of this study aids in creating a safer and more secure environment for students, faculty, and staff within educational institutions.

Keyword: Cyber security, educational management, Schools

1.0 Introduction

In recent years, Nigeria's education sector has witnessed rapid digital transformation. From adoption of Learning Management Systems (LMS) to the increased use of online assessments, cloud-based resources, and remote instruction—especially accelerated during the COVID-19 pandemic—educational institutions are more interconnected and technologically dependent than ever before. While these advancements offer tremendous opportunities for improving access, pedagogical innovation, efficiency, and global competitiveness, they also expose schools, colleges, and universities to a growing range of cyber threats.

The concept of educational management—encompassing policy formulation, curriculum delivery, record keeping, data privacy, personnel administration and infrastructure maintenance—relies

increasingly on digital platforms, large datasets, and networks. Yet, in many cases, cyber security considerations have been under-integrated or treated as secondary issues. In Nigeria, the vulnerabilities are multifold: inadequate infrastructure, limited human capacity, low awareness of cyber hygiene among educators and learners, and minimal regulatory enforcement. Scholarly studies have already documented incidents of data breaches, disruptions to virtual learning programs, challenges to the integrity of academic processes, and threats to stakeholder confidence.

Integrating cybersecurity into educational management is therefore not merely an IT concern, but a strategic imperative. Doing so can help safeguard personal and institutional data, ensure continuity of learning services, maintain trust in educational administration, and protect the reputational and financial assets of institutions. Moreover, as Nigeria strives to leverage education for national development, ensuring that its educational systems are resilient in the face of cyber risk is essential. This paper explores the importance of integrating cybersecurity within the structures and processes of educational management in Nigeria.

2.0 Literature Review

2.1 Concept of Educational Management

Educational management is all about how schools, colleges, and universities are run. It's the behind-the-scenes work that ensures everything functions smoothly—from creating school policies and hiring staff to managing budgets and evaluating performance. In simple terms, it's the application of good leadership and management practices to the education sector, helping institutions reach their goals effectively and efficiently.

Educational Management Involve:

Planning

This is where it all begins. School leaders set goals, design academic programs, plan budgets, and develop strategies to meet the needs of students and staff.

Organizing

Here, tasks and responsibilities are clearly assigned. Resources (like teachers, classrooms, and materials) are arranged in a way that supports smooth day-to-day operations.

Staffing

Educational institutions rely on dedicated professionals. Management involves recruiting the right people, supporting their development, and helping them thrive in their roles.

Leading (or Directing)

Good management requires strong leadership. This means guiding staff and students, inspiring them, and creating a positive environment where learning can flourish.

Monitoring and Control

To stay on track, schools need to measure their performance, assess learning outcomes, enforce rules, and hold everyone accountable for their roles.

Decision-making

Whether it's choosing a new teaching method or investing in technology, educational managers make informed decisions using data, feedback, and expert insights.

Importance of Educational Management include; ensures that resources—money, people, and materials—are used wisely; helps improve the quality of teaching and learning, keeps the school system organized, disciplined, and focused on its mission; makes it easier to implement new policies and educational reforms; encourages innovation and keeps education systems adaptable. Most importantly today, it helps schools respond to new challenges—like cybersecurity threats—by integrating modern tools and practices.

2.2 Concept of Cyber Security

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 (Ukhami, & Abdulsalam, 2024). For instance, sophisticated cyber criminals and nationstates, 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 Ukhami, et al 2024).

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 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 (Ogunode, Akpakwu, & Ochai, 2025). 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).

The objectives of school cyber security according to Ogunode, et al (2025) include; 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 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 cyberattacks.

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 cyberattacks.

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

The effects of integrating cyber-security in educational management in Nigeria. Thee paper is a position paper that adopted a systematic literature review-based method. The method allows to collect and review the related previous literature from various online sources. With the aid of digital platform, the researcher collected secondary information to generate knowledge on this topic from 2015-2025. The position paper followed qualitative narrative design method. The researcher has visited different online sites to collect the previous literature and analyze the effects of integrating cyber-security in educational management in Nigeria.. The previous findings are critically analyzed and presented in different themes as on the effects of integrating cyber-security in educational management in Nigeria (Adapted from Ogunode, 2025).

Inclusion and exclusion criteria

Inclusion

This output of the literatures on the effects of integrating cyber-security in educational management in Nigeria presents an in-depth study and result that can infer conclusion on the topic. The study includes: online publication; conference paper, journals sorted from from reputable international journals such as CEON, Elsevier, Hindawi, JSTOR, IEEE, Learn Techlib, SAGE, Nebraska and Springer (Adapted from Ogunode, 2025v).

Exclusion

Also, the literature review excludes information from edited books, preprints, monographs, information below 2015 and book chapters (Adapted from Ogunode, 2025).

4.0 Result and Discussion importance of integrating Cyber-security in Educational Management

Protection of Sensitive Information:

Cybersecurity is crucial in educational management as it ensures the protection of sensitive information such as student records, teacher information, and school financial data. With the integration of cybersecurity, schools can prevent data breaches and safeguard their sensitive information from cyber threats. Integrating cyber-security in educational management aids in the protection of sensitive information by implementing various measures such as data encryption, access controls, and monitoring systems. These measures ensure that only authorized individuals have access to sensitive information and that any unauthorized attempts are immediately detected and prevented (Ogunode, Ukozor, & Ugo-onyeka, 2025).. One of the key benefits of having cyber-security integrated in educational management is the protection of students' personal information. With the increasing use of technology in education, schools and educational institutions are collecting a vast amount of sensitive data from students, including personal information and academic records. This information needs to be protected from cyber threats such as hacking, data theft, and identity theft. Additionally, integrating cyber-security in educational management helps to prevent academic fraud (Howell & Lind, 2009). By implementing effective authentication and verification procedures, schools and educational institutions can ensure the integrity and authenticity of academic records. This is particularly important for higher education institutions where the credibility of academic records is crucial for employers and other educational institutions. Furthermore, cyber-security in educational management can also aid in protecting sensitive research and intellectual property (Mitigo 2024). With the digitization of research and online collaboration becoming the norm, the risk of data theft and intellectual property infringement increases. By implementing secure systems and protocols, schools and educational institutions can protect their research and intellectual property from cyber threats (Ikuero, 2022).

Prevention of Cyber Attacks:

As technology becomes more prevalent in education, the risk of cyber attacks increases. Integrating cybersecurity in educational management can help prevent these attacks and protect school systems from being compromised by hackers. The integration of cyber-security in educational management is essential for preventing cyber attacks (Ogunode, 2025). By incorporating cyber-security measures into the management of educational institutions, we can ensure the protection of sensitive information, such as student records and financial data, from cyber attacks. This also includes implementing secure network infrastructure and educating staff and students on safe internet practices. By prioritizing cyber-security in educational management, we can greatly reduce the risk of cyber attacks and safeguard the overall integrity of our educational institutions (StrongBox 2024).

Compliance with Data Privacy Regulations:

Many countries have implemented data privacy regulations, and schools must adhere to them. By incorporating cybersecurity in educational management, schools can ensure they are compliant with these regulations and avoid any legal consequences. Integrating Cyber-security in Educational Management is crucial for ensuring compliance with Data Privacy Regulations. This is because the education sector is increasingly reliant on technology and data for administration, teaching, and learning activities. With this reliance comes the risk of cyber threats and breaches of data privacy. By implementing strong cyber-security measures, educational institutions can better protect sensitive information and ensure compliance with data privacy regulations (Uwadia & Eti, 2018). One way in which integrating Cyber-security in Educational Management aids compliance with data privacy regulations is through the implementation of secure data storage and management systems. This includes utilizing encryption techniques to protect sensitive data, implementing secure servers and firewalls, and establishing strict access control protocols. By doing so, educational institutions can minimize the risk of data breaches and ensure that personal information is protected in accordance with data privacy regulations. Another way in which Cyber-security integration aids compliance is through the implementation of rigorous training and awareness programs for faculty, staff, and students. This ensures that all individuals within the educational institution are well-informed about cyber threats and how to prevent them. In addition, regular training helps to establish a culture of data privacy and security within the institution, reinforcing the importance of compliance with regulations (Nordlayer, 2023; Ukhamsi, & Abdulsalam, 2024). Integrating Cyber-security in Educational Management allows for the implementation of strict data privacy policies and procedures. These policies can outline the proper handling and sharing of personal data, as well as guidelines for reporting any potential breaches. By having these policies in place, educational institutions can demonstrate their commitment to compliance and their efforts to protect sensitive information (Ukhamsi & Abdulsalam, 2024).

Protecting Online Learning Platforms:

With the shift towards online learning, schools have become more reliant on digital platforms. Cybersecurity can help protect these platforms from being hacked, ensuring a smooth and secure experience for both students and teachers. The integration of cyber-security in educational management is essential in protecting online learning platforms. With the increasing reliance on technology in the education sector, it has become necessary to ensure the safety and security of online learning platforms (Nwachukwu, 2021). Cyber-security helps in this aspect by implementing measures to prevent unauthorized access, data breaches, and other cyber threats. It also involves proactive monitoring and quick response to any potential threats. One of the main advantages of integrating cyber-security in educational management is that it helps in protecting sensitive data. Online learning platforms contain a vast amount of personal information, such as student records, financial information, and confidential research data. Cyber-security measures,

such as encryption and user authentication, ensure that this data is kept safe from cyber attacks. Additionally, cyber-security in educational management helps in protecting the integrity of online learning platforms (Khodzhanovna, 2023; Cassim, 2017). This means ensuring that the information and resources available on the platform are accurate, authentic, and tamper-proof. Cyber-security measures such as firewalls, intrusion detection systems, and regular system updates play a crucial role in maintaining the integrity of online learning platforms. Moreover, the integration of cyber-security in educational management aids in protecting the availability of online learning platforms. This means ensuring that the platform is up and running without any disruptions. Cyber-security measures, such as backup and disaster recovery systems, help in mitigating the impact of any potential cyber attacks or technical failures, ensuring that students can continue their education without any interruptions (Greenwald, 2014).

Building a Culture of Cybersecurity Awareness:

By integrating cybersecurity in educational management, schools can promote a culture of cybersecurity awareness among students, teachers, and staff. This can help educate them about the potential risks and how to protect themselves and the school from cyber threats. It also teaches responsible use of technology, ensuring students are equipped with the necessary skills to navigate the digital world safely (Editorial Team 2024).

4.1 Finding

The paper revealed that integration of cyber security into educational management in Nigeria will lead protection of sensitive information, prevention of cyber-attacks, compliance with data privacy regulations, protecting online learning platforms and building a culture of cybersecurity awareness.

4.2 Conclusion

The paper examined the importance of integrating cybersecurity within the structures and processes of educational management in Nigeria. The paper concluded that integration of cyber security into educational management in Nigeria will lead protection of sensitive information, prevention of cyber-attacks, compliance with data privacy regulations, protecting online learning platforms and building a culture of cybersecurity awareness.

References

Cassim, F. (2011) Addressing the growing spectre of cybercrime in Africa: evaluating measures adopted by South Africa and other regional role players. CILSA XLIV 123-138

DOD (2025). What is cyber security education?
<https://www.toolbot.ai/apps/AI%20Abstracteer?desc=A%20tool%20that%20generates%20>

[academic%20abstracts%20from%20user%20input&placeholder=Enter%20a%20topic%20for%20your%20abstract%20.](#)

Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York, NY: Metropolitan Books/Henry Holt.

Editorial Team (2024). Cyber security training <https://www.indeed.com/career-advice/finding-a-job/cyber-security-training>

Howell, J. & Lind, J. (2009). *Counter-Terrorism, Aid and Civil Society: Before and After the War on Terror*. Basingstoke, UK: Palgrave Macmillan. ISACA, (2014).

Ikuero, F. E. (2022). Preliminary Review of Cybersecurity Coordination in Nigeria. *Nigerian Journal of Technology (NIJOTECH)*, 41(3),pp.521-526

Khodzhanovna, S, K (2023).cybersecurity is an important information security principle. *Best journal of innovation in science, research and development*,02(07), 136-169.

Mitigo (2024). What is cyber security training? [https://mitigogroup.com/cyber-security-wiki/whatis-cybersecuritytraining/#:~:text=Cybersecurity%20training%20is%20used%20to,\)C%20networks%20and%20cloud%20services](https://mitigogroup.com/cyber-security-wiki/whatis-cybersecuritytraining/#:~:text=Cybersecurity%20training%20is%20used%20to,)C%20networks%20and%20cloud%20services).

Nwachukwu, (2021). “Nigeria: A Failing State Teetering on the Brink.” *The Punch News*. 19 May.

Nordlayer,(2023) “Cybersecurity in Education: Back to School, Back to Risks. [Online].

Available: <https://nordlayer.com/blog/cybersecurity-challenges-in-education/>

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

Ogunode, N., J. Akpakwu, F., O & Ochai, D., P. (2025). Cyber Security and School Management in Nigeria. *International Journal of Business, Law and Political Science*, 2(5),123-133

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.

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>

- StrongBox IT, (2024). “The Role of Cybersecurity in Schools and Universities.” <https://www.linkedin.com/pulse/role-cybersecurity-schoolsuniversitiesstrongbox-it-pvt-ltdjpdte#:~:>
- 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.innoscience.com/index.php/ijnras/article/view/41>
- 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.
- 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.
- 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.
- Vain, C (2025). Strategies for Digital Safety and Cybersecurity in Schools
<https://cpdonline.co.uk/knowledge-base/safeguarding/strategies-digital-safety-cybersecurity-schools>