AJLLSE GLOBAL RESEARCH NETWORK

AMERICAN Journal of Language, Literacy and Learning in STEM Education
Volume 3, Issue 8, 2025 ISSN (E): 2993-2769

Cyber Security and Educational Institution in Nigeria: Benefits and Challlenges

Okwori Favour Osato
General Administration Staff Welfare Department, Ambrose Alli University, Ekpoma

Olowonefa Jethro Abiodun. Ph.D
Educational Management, Faculty of Education, University Of Abuja, Nigeria

Chioma Fortune Olali PhD
River state university, Department of educational Management, Faculty of Education

Victor Olugbenga Ayoko
Department of Educational Foundations, Faculty of Education, Open University of Faculty of Education, National, Nigeria

Abstract: *This study discussed the import of cyber security in the educational institution in Nigeria. The paper also looked at the challenges militating against development of cyber security in the institutions. The paper depend on secondary data. The secondary data were collected from online and print resources. The paper identified protection of students and staff data, stable academic programme, stable school administration, stable virtual learning programme and confidence in school integrity as the benefits of cyber security development in the Nigeria' educational institutions. The paper also identifies inadequate funding, inadequate infrastructure, technological advancement, poor training and shortage of cyber security professionals as challenges militating against cyber security development in educational institutions in Nigeria. Based on the findings, the study recommends the following: the government should direct all educational institutions to embark on cyber security programme that will ensure safety of students and staff data from their part. The federal and state government should provide special funding for the implementation of cyber security programme in all public institutions across Nigeria. The government should provide cyber infrastructure facilities across the states and local government to support effective implementation of cyber security programme.*

Key words: *Benefits, Cyber security, Education.*

1.0 Introduction

Educational institutions across the globe are facing the problem of cyber-crime. For instance, Johnson in (2023) reported that the management of Babcock University has said that the school's website has been hacked by some unknown persons. The school management confirmed this development in a statement signed by the Director, Communication & Marketing of the institution, Dr Joshua Suleiman, on Wednesday. The statement read in part, "The public is hereby notified that the Babcock University management information system has been violated by suspected unscrupulous persons with intent to embarrass, deceive and defraud unsuspecting university clients and stakeholders. "The criminals had gained unauthorised, illegitimate, illicit access to some of the university's client

inconsequential records from the front-end server of the university and threatened dire consequences if the university does not reach out to them, they also claim that the university's sensitive information had been compromised.

Also, Ogwo (2025) reported that not than 20 people were arrested for computer-based test (CBT) hacking across the nation in crackdown exercise in the 2025 Unified Tertiary Matriculation Examination (UTME) conducted by the Joint Admission and Matriculation Board (JAMB). According to report, security agents have detained over 20 individuals in Abuja in connection with the large-scale breach of the 2025 computer-based examination system of JAMB. The arrests were carried out by operatives of the Department of State Services (DSS) and the Nigerian Police Force.

The apprehended suspects are reportedly members of a cybercriminal syndicate comprising more than 100 individuals who are notorious for targeting the digital infrastructure of key examination bodies, including JAMB and the National Examinations Council (NECO). According to security insiders, the culprits admitted to deliberately compromising JAMB's computer-based test platform in a bid to damage the board's credibility and create doubt around the effectiveness of CBTs in future WAEC and NECO assessments (Ogwo, 2025; Muhammad & Yusuf 2025)

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

2.0 Review of Literature

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 (Schneier and Bruce, 2016).

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 (Muhammad, 2016; Nwachukwu 2021).

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 (Muhammad & Bashir, 2021; Khodzhanovna, 2023).

Cyber Security 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). Cyber security according to Ogunode, Akpakwu, & Ochai, (2025) is the best practices that individuals or organisations can put in place to reduce the risk of an intrusion by an insider or outsider obtaining access to private information. Preventing attacks and damage to devices used by individuals and organisations, including computers, laptops, tablets, smartphones, and handhelds, as well as the internet services they use both at work and online, is the primary objective of cyber security. The objectives of school cyber security include creating a strong security posture against attacks that seek to access, alter, erase, destroy, or extort sensitive data and school or user systems, protecting student information from the public domain, and defending school confidential data from attacks. Cybersecurity is a structured approach to complete data protection (Ogunode, et al 2025). 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 local school districts. Schools need enterprise-class security measures and hardware-enabled security to help protect their students, faculty, and data from cyberattacks (Intel Team 2024).

2.1 Common Types of Cyber Attacks in Cyber Security

Saini (2025) listed the following as the types of cyberattacks in cyber security

1. Phishing

Phishing is a social engineering attack where attackers impersonate legitimate entities to deceive individuals into sharing sensitive information, such as usernames, passwords, and financial details. These attacks often occur through fraudulent emails, fake websites, or instant messages that trick victims into clicking malicious links or downloading infected attachments. Advanced phishing techniques include spear phishing (targeted attacks) and whaling (attacks on high-profile individuals like executives).

2. Malware

Malware (malicious software) is designed to harm or exploit computer systems, networks, or devices. Common types of malware include:

1. Viruses: Attach to legitimate programs and spread when executed.

2. Trojans: Disguised as legitimate software but perform malicious activities.

3. Ransomware: Encrypts files and demands ransom for decryption.

4. Spyware: Secretly gathers user information, such as login credentials.

5. Worms: Self-replicating malware that spreads across networks without human intervention.

3. DoS & DDoS Attacks

A Denial-of-Service (DoS) attack aims to overwhelm a system, server, or network by flooding it with excessive requests, causing slowdowns or crashes.

A Distributed Denial-of-Service DDoS attack is a more severe version where multiple compromised computers (botnets) coordinate an attack, making it harder to mitigate. These attacks disrupt online services, financial institutions, and e-commerce platforms.

4. Man-in-the-Middle (MitM) Attack

In a MitM attack, an attacker intercepts and manipulates communication between two parties without their knowledge. Common MitM attack methods include:

Session Hijacking: Stealing active user sessions to gain unauthorized access.

Wi-Fi Eavesdropping: Intercepting unencrypted data on public Wi-Fi networks.

HTTPS Spoofing: Redirecting users to fake HTTPS sites to capture credentials.

5. SQL Injection

SQL Injection is a code injection attack in which attackers insert malicious SQL queries into the input fields of web applications to manipulate databases. This allows hackers to retrieve, modify, or delete sensitive data, such as user credentials or financial records.

Example: Entering ' OR '1'='1 into a login field to bypass authentication.

Master the latest tools and techniques to protect systems from evolving threats.

6. Cross-Site Scripting (XSS)

XSS attacks occur when an attacker injects malicious scripts into a legitimate website, which executes in a user's browser.

1> Stored XSS: The script is permanently stored on the website (e.g., in comment sections).

2. Reflected XSS: The script is temporarily executed via a crafted URL.

3. DOM-Based XSS: Manipulates the browser's document object model (DOM).

7. Zero-Day Exploit

A Zero-Day exploit targets previously unknown vulnerabilities in software before the vendor releases a fix or patch. Attackers exploit these security flaws to execute unauthorized commands, steal data, or install malware.

8. Brute Force Attack

A brute force attack is a trial-and-error method to guess login credentials or encryption keys by systematically trying all possible combinations.

Dictionary Attack: Uses precompiled lists of common passwords.

Credential Stuffing: Uses previously leaked credentials to gain access to multiple accounts.

9. Credential Stuffing

Credential stuffing occurs when attackers use stolen username-password combinations from past data breaches to gain unauthorized access to other accounts.

Why it works? Many users reuse passwords across multiple platforms.

10. Insider Threats

Insider threats originate from employees, contractors, or partners accessing an organization's systems. These threats can be:

Malicious (Disgruntled Employees): Deliberate sabotage, data theft, or leaking confidential information. Negligent (Careless Employees): Clicking on phishing emails, weak password practices, or misconfiguring security settings. Compromised (Social Engineering Victims): Employees unknowingly grant access to attackers.

3.0 Method

It is a systematic literature review-based report. It has collected and reviewed the related previous literature from various online sources. It has collected secondary information to generate knowledge on this topic. It has followed the qualitative narrative design. The researcher has visited different online sites to collect the previous literature and analyze the benefits of cyber security in educational institutions Nigeria.

Inclusion and exclusion criteria

This research article presents the results of an in-depth study that included conference and article. It excludes information from edited books, preprints, monographs, and book chapters.

4.0 Result and Discussion on Benefits of Cyber Security

The benefits of cyber security to educational management according to Ogunode (2025) includes;

A) Protection of students and staff data

The school keeps both students and staff vital information that are supposed to be personal data. These information are required by the schools as a criterial for admission or for employment. These information may include bank details of the staff and students bio-date. Access to these details by hackers can lead ransom collection or bullying in the part of the students. Application of cyber security programme by the schools can help the schools mitigate against hackers and to loss the data to an unauthorized party. AAA (2025) observed that cyber security helps to safeguard against cyber attacks and data breaches. Educational institutions in Nigeria often hold a vast amount of personal and sensitive student information, including academic records and financial details. With cyber security measures in place, these institutions can protect this data from malicious attacks and unauthorized access.

B) Stable academic programme

One of the core responsibilities of the school management is to ensure stable academic programme for both students and staff. Maintaining a stable academic programme demands that the school put everything under her control. Factor like hacking into school financial account with the financial institutions by third party will affects smooth running of the schools that will directly affects stable academic programme or the hacking of school data that have link with e-school resources and materials. This can also disrupts the academic programme of the schools but with deployment of cyber security system in the school such incidences can be minimized.

C) Stable school administration

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

D) Stable virtual learning programme

Most schools in Nigeria have adopted blended learning style that permitted both off-line and online learning process. The blended learning style demands the school to prepare e-learning resources to support the virtual aspect of the learning processes which include the use of e-libraries and e-platforms. The e-libraries and e-resources material or data can be hacked by unauthorized party if the necessary measure are not put in place by the school management. Stable virtual learning can be ensure in the school via deployment of cyber security system and regular update of the system. 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 (Ogunode, Akpakwu, & Ochai 2025; StrongBox IT, 2024; Mitigo 2024).

E) Confidence in school integrity

School stakeholders that includes students, parents, teachers, government, non-government organizations and private institutions wants schools that are reliable and have integrity to partner with in the areas of provision of educational services. The trust, confidence and integrity of the school implies that they want schools that can be accountable in the areas of resources allocation that required

presentation of data on every input of the school. The degree and extent to which theses schools can protect these data and present them at a single demands will make the stakeholder trust the school management. Deployment of cyber security measures by the schools can help them build this trust and confident on their stakeholders in Nigeria. In addition to this, cyber security can also help to build trust and confidence among stakeholders, including students, parents, and teachers. With a secure platform, students can feel safe in their online interactions, and parents can rest assured that their child's information is protected. This trust can also extend to potential students and parents, as they can have confidence in the institution's commitment to safeguarding their data (AAA 2025; CISCO, 2023).

Challenges militating against Security cyber

i) Inadequate Funding:

Inadequate funding is a major problem hindering the development of cyber security in educational institutions in Nigeria. The budgetary allocation to education which include cyber security programme in Nigeria is not adequate to implement the develop cyber security in the institutions. The allocation of financial resources to primary schools, secondary schools, tertiary institutions and educational institutions such as agencies and commissions is insufficient, leading to a lack of basic equipment, infrastructure, and personnel for the implementation of the cyber security programme.

ii) Inadequate Infrastructure

Another problem hindering the development of cyber security in Nigeria' educational institutions is lack of adequate cyber security infrastructure facilities. These facilities are not adequate to support the teachers and personnel to deliver the lectures in the classrooms and protect institutions data. The shortage of facilities have also affected development of cyber security in schools, agencies and commission.

iii) Technological Advancement

The biggest challenge in cybersecurity today in the various educational institutions in Nigeria is the ever-changing nature of technology. Cybercriminals are constantly inventing new technologies, techniques and strategies to exploit vulnerabilities in networks and systems. Moore (2025) noted that AI-powered cyber-attacks are emerging as a significant challenge in the cybersecurity arena. Cybercriminals are using artificial intelligence to elevate the sophistication and impact of their attacks, making them increasingly elusive and harder to detect. These AI-driven threats can automate vulnerability identification, craft convincing phishing schemes and even adapt in real-time to circumvent security measures. The dynamic nature of AI means traditional defenses may no longer be sufficient. This calls for a proactive and innovative approach to cybersecurity. Organizations must prioritize investment in AI-driven security solutions and continuously refine their strategies to stay ahead of these rapidly evolving threats.

vi) Poor training

Poor training and retraining programme for cyber security personnel has also contributed to poor development of cyber security in educational institutions in Nigeria. Chand, (undated) viewed training constitutes a basic concept in human resource development. It is concerned with developing a particular skill to a desired standard by instruction and practice. Training is a highly useful tool that can bring an employee into a position where they can do their job correctly, effectively, and conscientiously. Training is the act of increasing the knowledge and skill of an employee for doing a particular job. The operation of cyber security facilities in the schools, agencies and commission demands constant training programme for the personnel in charge of operation of cyber security facilities. It is unfortunate that most operator of cyber security facilities in the educational institutions are not constantly been exposed to training programme which have affected the teaching and learning of cyber security education.

v) Shortage of cyber security professionals

Another problem militating against development of cyber insecurity in the educational institutions in Nigeria is the shortage of professional cyber security. The inability of these institutions to access expertise and professionals that will handle the cyber security management in the institutions have affected the development of cyber security in the institutions. The cybersecurity workforce shortage has reached a critical level, exacerbated by challenging economic conditions that have led to increased resource reductions.

Findings

This study revealed the import of cyber security in the educational institution in Nigeria. The paper identified protection of students and staff data, stable academic programme, stable school administration, stable virtual learning programme and confidence in school integrity as the benefits of cyber security development in the Nigeria' educational institutions. The paper also identifies inadequate funding, inadequate infrastructure, technological advancement, poor training and shortage of cyber security professionals as challenges militating against cyber security development in educational institutions in Nigeria.

Conclusion and Recommendations

This study discussed the import of cyber security in the educational institution in Nigeria. The paper identified protection of students and staff data, stable academic programme, stable school administration, stable virtual learning programme and confidence in school integrity as the benefits of cyber security development in the Nigeria' educational institutions. The paper also identifies inadequate funding, inadequate infrastructure, technological advancement, poor training and shortage of cyber security professionals as challenges militating against cyber security development in educational institutions in Nigeria.

Based on the findings, the study recommends the following: the government should direct all educational institutions to embark on cyber security programme that will ensure safety of students and staff data from their part. The federal and state government should provide special funding for the implementation of cyber security programme in all public institutions across Nigeria. The government should provide cyber infrastructure facilities across the states and local government to support effective implementation of cyber security programme. The government should direct the ministry of education to organize training for school administrators and teachers on the importance of cyber security in educational institutions. Private institutions should support by providing capacity building for both teachers and students on the importance of cyber security in school.

References

1. AAA (2025). Importance of cyber security in educational management in Nigeria. https://www.toolbot.ai/apps/AI%20Abstracteer?desc=A%20tool%20that%20generates%20academic%20abstracts%20from%20user%20input&placeholder=Enter%20a%20topic%20for%20your%20abstract%20
2. CISCO, (2023). "What is Cyber Security?". [Online]. Available: https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html
3. Frank, I. and Odunayo, E. (2013) "Approach to cyber security issues in Nigeria: challenges and solution''
4. Garba, A.A. and Bade, A.M. (2021). "The Current State of Cybersecurity Readiness in Nigeria organizations'', *Educational Research (IJMCER),* 3(1), 2021, pp 154-162.
5. Johnsom, H. (2023). Babcock-university-confirms-hack-of-school-website https://punchng.com/babcock-university-confirms-hack-of-school-website/
6. Nelson, N,. J. (2025). Nigeria Education Sector Vulnerable to hackers. https://comnavig.com/blog/nigeria-education-sector-vulnerable-to-hackers---by-nsikak-joseph-nelson-ceo-silex-secure-

7. NOUN (2012). Issues and problem in higher education in Nigeria. Lagos.
8. Novikava, A (2024). Cybersecurity in education: back to school, back to risks https://nordlayer.com/blog/cybersecurity-challenges-in-education/
9. Khodzhanovna, S,. K. (2023). Cybersecurity is an important information security principle. *Best journal of innovation in science, research and development* ,02(07),136-139.
10. Moore, M. (2025) Top Cybersecurity Threats to Watch in 2025 https://onlinedegrees.sandiego.edu/top-cyber-security-threats/
11. Muhammad, A. S. (2016) The Role of Religion in Conscience Reawakening of the Youth. Journal Of Humanities And Social Science (IOSR-JHSS) Volume 21, Issue 7, Ver. 1 PP 14-19
12. Muhammad, A. S, & Bashir, A. I. **(**2021) Mosque as an Essential Combat in the Face of Covid-19: A Critical Discourse from the Islamic Viewpoint'' *Gadau Journal of Arts and Humanities*, Faculty of Arts, Bauchi State University, Gadau. Vol, 4, No 3. PP: 180-194.
13. Muhammad, A.S. & Yusuf A.J. (2025). Persistence and its Impact on Minor Sins among Muslims in Kwara State Nigeria. *Spanish Journal of Innovation and Integrity*, *44*, 136–146.
14. Nwachukwu, (2021). "Nigeria: A Failing State Teetering on the Brink." The Punch News. 19 May.
15. 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*, IJBLPS, 2,(5), 123-133
16. 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),146-153.
17. Ogwo, C. (2025). 2025-utme-over-20-arrested-for-cbt-hacking https://businessday.ng/news/article/2025-utme-over-20-arrested-for-cbt-hacking/
18. 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
19. Saini, K (2025). Types-of-cyber-attacks https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks
20. 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), pp. 351-354,