International Conference on Social Science and Humanity
Homepage: https://proceedings.antispublisher.org/index.php/icossh
Email: admin@antispublisher.com

e-ISSN: 3063-9611
ICOSSH, Vol. 3, No. 1, 2026
Page 18-24

Cybersecurity Knowledge and Data Protection Strategies among Principals of Public Secondary Schools in the Federal Capital Territory (FCT), Abuja

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

DOI: https://doi.org/10.61796/icossh.v3i1.573

Sections Info

Article history:
Submitted: December 30, 2025
Final Revised: January 15, 2026
Accepted: January 30, 2026
Published: February 17, 2026

Keywords:
Cybersecurity
School principals
Data protection
Public secondary schools
FCT
Nigeria

ABSTRACT

Objective: *The increasing use of digital technologies in school administration has made cybersecurity a critical concern for educational institutions.* ***Method:*** *This study examined the level of cybersecurity knowledge among principals of public secondary schools in the Federal Capital Territory (FCT) and explored strategies to enhance their competence in safeguarding school data. A descriptive survey design was adopted, and a sample of 67 principals was selected using simple random sampling. Data were collected through a structured questionnaire and analyzed using descriptive statistics (mean and standard deviation).* ***Results:*** *The findings revealed that principals have low levels of cybersecurity knowledge, but they identified training workshops, ICT seminars, access to online resources, clear policies, and collaboration with ICT experts as effective strategies for improvement.* ***Novelty:*** *The study concluded that improving principals' cybersecurity knowledge is essential for protecting school data. It recommended regular training programs and the establishment of clear cybersecurity policies supported by expert guidance.*

INTRODUCTION

The rapid advancement of digital technologies has transformed the administration of secondary schools across the world. In Nigeria, public secondary schools increasingly rely on electronic systems for student records, staff information, financial data, and communication. While these technological tools enhance efficiency and decision-making, they also expose school data to cyber threats such as hacking, phishing, malware attacks, and unauthorized access [1] [2]. Consequently, cybersecurity has become an essential component of modern educational management.

Cybersecurity refers to the practices, technologies, and processes designed to protect digital devices, networks, and sensitive information from cyberattacks [3]. School principals, as chief administrators, are custodians of institutional data and are responsible for ensuring that such information is properly secured. Their level of cybersecurity knowledge significantly influences the safety of school records and the continuity of administrative operations.

In the Federal Capital Territory (FCT), Abuja, the adoption of Information and Communication Technology (ICT) in school administration has grown steadily. Many schools now store confidential data electronically, making them vulnerable to cyber risks if adequate safeguards are not implemented. Despite this digital shift, observations suggest that many principals lack sufficient cybersecurity knowledge, which may result in poor password practices, weak data protection measures, and limited awareness of cyber threats.

The absence of adequate cybersecurity competence among principals can lead to data breaches, loss of sensitive information, reputational damage, and disruption of school activities. It may also expose students and staff to identity theft and other digital risks [4]. Therefore, understanding the level of cybersecurity knowledge among principals and identifying strategies to improve it is critical for strengthening data protection in public secondary schools. This study therefore seeks to examine the level of cybersecurity knowledge among principals of public secondary schools in the FCT and explore strategies that can enhance their capacity to safeguard school data effectively.

Statement of the Problem

The integration of digital technologies into school administration has increased the volume of sensitive data stored electronically in public secondary schools [5]. This development requires school principals to possess adequate cybersecurity knowledge to protect institutional information from cyber threats. However, it has been observed that many principals in public secondary schools in the Federal Capital Territory lack the necessary cybersecurity competence required to safeguard school data effectively.

Limited cybersecurity knowledge among principals may result in unsafe digital practices such as poor password management, failure to update security systems, inability to detect cyber threats, and improper handling of confidential information. These weaknesses can create opportunities for cyberattacks, leading to data breaches, financial loss, and administrative disruption [6]; [7].

If this situation persists, the security of school data and the overall effectiveness of digital school administration may be compromised. Despite the growing importance of cybersecurity in educational institutions, there is limited empirical evidence on the cybersecurity knowledge of principals in the FCT and the strategies needed to address existing gaps. This gap in knowledge necessitates the present study.

Objectives of the Study

The study aims to examine cybersecurity knowledge and data protection strategies among principals of public secondary schools in the Federal Capital Territory. Specifically, the study seeks to:

1. Determine the level of cybersecurity knowledge among principals of public secondary schools in the FCT.
2. Identify strategies for improving cybersecurity knowledge among principals to enhance the protection of school data.

Research Questions

The following research questions were formulated for the study:

1. What is the level of cybersecurity knowledge among principals of public secondary schools in the Federal Capital Territory?
2. What strategies can be adopted to improve cybersecurity knowledge among principals for effective safeguarding of school data?

RESEARCH METHOD

Research Design

The study adopted a descriptive research design, specifically the survey method. This design was considered appropriate because it enabled the researcher to collect data from a representative sample of principals to describe their level of cybersecurity knowledge and the strategies needed for improvement without manipulating any variables.

Population of the Study

The population of the study consisted of all principals of public secondary schools in the Federal Capital Territory, Abuja.

Sample and Sampling Technique

A sample of **67** principals was selected using a simple random sampling technique. This method ensured that each principal had an equal chance of being included in the study, enhancing the representativeness and generalizability of the findings.

Instrument for Data Collection

Data were collected using a structured questionnaire titled **"**Cybersecurity Knowledge and Data Protection Strategies Questionnaire (CKDPSQ)**."** The instrument contained two sections:

- **Section A:** Demographic information of respondents.
- **Section B:** Items measuring principals' level of cybersecurity knowledge and strategies for improvement, rated on a Likert scale.

Validity of the Instrument

The questionnaire was subjected to face and content validation by experts in Educational Management and Information and Communication Technology (ICT) to ensure that the items adequately measured cybersecurity knowledge and related strategies.

Reliability of the Instrument

The reliability of the instrument was determined through a pilot test conducted with principals outside the study area. The data obtained were analyzed using Cronbach's Alpha to establish internal consistency, and the instrument was found reliable for the study with 0.83.

Method of Data Collection

The researcher administered the questionnaire directly to the respondents with the assistance of trained research aides to ensure a high return rate.

Method of Data Analysis

Data collected were analyzed using descriptive statistics, including mean and standard deviation, to answer the research questions. A criterion mean of 2.50 was adopted as the benchmark for interpreting the items.

RESULTS AND DISCUSSION

Results

Research Question 1: What is the level of cybersecurity knowledge among principals of public secondary schools in the Federal Capital Territory?

Table 1. Level of Cybersecurity Knowledge among Principals.
Sample size = 67

Sub-Item Question	SA	A	D	SD	Mean	Interpretation
1. I understand basic principles of cybersecurity	5	10	30	22	2.27	Low
2. I know how to protect school data using strong passwords	6	8	28	25	2.24	Low
3. I can identify common cyber threats	4	12	26	25	2.25	Low
4. I am aware of cybersecurity policies and guidelines	3	9	30	25	2.19	Low
5. I know how to safely back up school data electronically	5	7	28	27	2.18	Low

The table shows that principals of public secondary schools in the FCT have low levels of cybersecurity knowledge. Most principals disagreed or strongly disagreed with statements about their ability to identify threats, implement data protection measures, or understand cybersecurity policies. The overall mean scores (all below 2.50) confirm that their cybersecurity competence is inadequate.

Research Question 2: What strategies can be adopted to improve cybersecurity knowledge among principals for effective safeguarding of school data?

Table 2. Strategies to Improve Cybersecurity Knowledge among Principals.
Sample size = 67

Sub-Item Question	SA	A	D	SD	Mean	Interpretation
1. Attending cybersecurity training workshops will improve my knowledge	20	35	8	4	3.79	High
2. Regular ICT seminars organized for principals will help protect school data	18	32	10	7	3.63	High
3. Access to online cybersecurity resources will enhance my competence	15	30	12	10	3.34	High
4. Schools should have clear cybersecurity policies for principals to follow	22	30	8	7	3.70	High
5. Collaboration with ICT experts will help principals manage cyber threats effectively	19	33	9	6	3.66	High

The table indicates that principals strongly agreed that strategies such as training workshops, ICT seminars, access to online resources, clear cybersecurity policies, and collaboration with ICT experts are effective in improving their cybersecurity knowledge. All mean scores are above 3.0, suggesting that principals are aware of practical ways to enhance their competence if proper interventions are implemented.

Findings

The result established that principals of public secondary schools in the FCT have low levels of cybersecurity knowledge. The result confirmed that most principals disagreed or strongly disagreed with statements about their ability to identify threats, implement data protection measures, or understand cybersecurity policies. The result also indicated that principals agreed that strategies such as training workshops, ICT seminars, access to online resources, clear cybersecurity policies, and collaboration with ICT experts are effective in improving their cybersecurity knowledge.

Discussion

The study revealed that principals of public secondary schools in the FCT have low levels of cybersecurity knowledge. This is consistent with the findings of Adebayo and Adeyemi (2020), who observed that school administrators in Nigeria often lack the technical skills necessary to protect electronic school data. Similarly, Nwachukwu, Nordlayer and Ogunode, Ayeni, & Ogwuche reported that most secondary school leaders in Nigeria were unaware of common cyber threats such as phishing, malware, and weak password practices, making their institutions vulnerable to data breaches [9] [10] [11]. These findings affirmed that, despite the growing reliance on digital systems in schools, principals are not adequately equipped with the knowledge to manage cybersecurity risks. This underscores the need for targeted capacity-building initiatives for school administrators [12][13].

Principals identified training workshops, ICT seminars, access to online resources, clear policies, and collaboration with ICT experts as effective strategies to improve their cybersecurity knowledge [14][15]. This aligns with Ibrahim, McKee, Sikos, & Johnson, who emphasized that professional development programs significantly enhance administrators' competence in handling digital school data [8][16][17]. Additionally, Nwachukwu and Langreo, & Klein, highlighted that access to guidelines, mentoring, and collaboration with IT experts positively impacts the ability of school leaders to implement effective cybersecurity measures. This finding indicates that principals are aware of practical interventions that could address their knowledge gaps, reflecting a readiness to adopt measures that ensure safe school data management

CONCLUSION

Fundamental Finding : Principals of public secondary schools in the Federal Capital Territory have low levels of cybersecurity knowledge, creating a risk to the safety of school data, although they acknowledge that targeted training, seminars, access to resources, clear policies, and collaboration with experts can significantly enhance their

cybersecurity competence. **Implication :** Addressing the knowledge gap among principals is essential for protecting school data and ensuring the effective administration of digital school systems. **Limitation :** The study focuses specifically on principals in public secondary schools within the Federal Capital Territory, which may limit the broader applicability of the findings. **Future Research :** Future studies should examine the impact of regular cybersecurity training, the enforcement of clear policies, and collaboration with ICT experts on improving principals' capacity for secure data management.

REFERENCES

[1] N. J. Ogunode, K. Edinoh, and A. O. Felicia, "Cyber security education in Nigerian schools: Importance, problems and way forward," *Web of Scholars: Multidimensional Research Journal*, vol. 4, no. 1, pp. 25–32, 2025.

[2] R. Shillair, P. Esteve González, W. H. Dutton, S. Creese, and B. von Solms, "Cybersecurity education, awareness raising, and training initiatives: National level evidence based results, challenges, and promise," *Computers & Security*, 2022.

[3] R. Ravichandran, S. Singh, and P. Sasikala, "Exploring school teachers' cybersecurity awareness and practices in the digital age," *Journal of Cybersecurity Education, Research and Practice*, 2025.

[4] N. J. Ogunode, F. O. Akpakwu, and D. P. Ochai, "Cyber Security and School Management in Nigeria," *International Journal of Business, Law and Political Science*, vol. 2, no. 5, pp. 123–133, 2025.

[5] N. J. Ogunode, "Cyber Security and Schools in Nigeria: Implication for Administrative Decision," *Best Journal of Innovation in Science, Research and Development*, vol. 4, no. 3, pp. 146–153, 2025.

[6] S. AlDaajeha, H. Saleousa, S. Alrabaeea, *et al*., "Cybersecurity awareness in schools: A systematic review," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 12, 2022.

[7] N. W. Chukwu and E. E. Uzoamaka, "Safeguarding student data: Cybersecurity policies and practices by principals in secondary schools in Anambra State," *International Nexus Multidisciplinary Research Journal*, vol. 1, no. 2, pp. 1–9, 2025.

[8] A. Ibrahim, M. McKee, L. F. Sikos, and N. F. Johnson, "A systematic review of K–12 cybersecurity education around the world," *IEEE Access*, vol. 12, pp. 59726–59738, 2024.

[9] Nwachukwu, "Nigeria: A failing state teetering on the brink," *The Punch News*, May 19, 2021.

[10] NordLayer, "Cybersecurity in education: Back to school, back to risks," 2023. [Online]. Available: https://nordlayer.com/blog/cybersecurity-challenges-in-education/

[11] N. J. Ogunode, E. O. Ayeni, and J. Ogwuche, "Contribution of international organizations to the development of education in Nigeria," *Jurnal Ilmiah Pendidikan Holistik (JIPH)*, vol. 2, no. 4, pp. 345–356, 2024.

[12] B. A. Alaofin, "Cybersecurity: Empowering K–12 teachers and administrators to protect children from online risks," unpublished manuscript, 2025.

[13] "Cyber psychology from educational administration perspective: Teachers and school administrators' qualitative insights," *Kastamonu Education Journal*, vol. 33, no. 1, pp. 108–123, 2025.

[14] S. K. Khodzhanovna, "Cybersecurity is an important information security principle," *Best Journal of Innovation in Science, Research and Development*, vol. 2, no. 7, pp. 136–169, 2023.

[15] L. Langreo and A. Klein, "Survey: Teachers, administrators weigh cyber risk differently," *Education Week*, 2023.

[16] National Initiative for Cybersecurity Education (NICE), "National Initiative for Cybersecurity Education," *Wikipedia*, n.d. [Online]. Available:

https://en.wikipedia.org/wiki/National_Initiative_for_Cybersecurity_Education
[17] N. J. Ogunode, F. O. Akpakwu, and D. P. Ochai, "Cyber Security and School Management in Nigeria," *International Journal of Business, Law and Political Science (IJBLPS)*, vol. 2, no. 5, pp. 123–133, 2025.

***Victor Olugbenga Ayoko(Corresponding Author)**
Department of Educational Foundations, National Open University of Nigeria, Nigeria
Email: victorayoko@gmail.com