VOL. 12 NO. 8,
MAY, 2026
E-ISSN 3026-8893
P-ISSN 3027-1061

African Scholar Publications & Research International
www.africanscholarpub.com

Journal of Education Research and Library Practice (JERLP)

Evaluating Cybersecurity Infrastructure in Nigerian Higher Education Institutions

Binitie Amaka Patience; & Iyawa, Jane Ifeyinwa Bieniose
Computer Science Department, Federal College of Education (T), Asaba.
Corresponding Author: philpat4ure@gmail.com
DOI: https://doi.org/10.70382/ajerlp.v12i8.087

Abstract

The rapid digital transformation in Higher Education Institutions (HEIs) has heightened vulnerability to cyber threats like ransomware, phishing, and data breaches, yet cybersecurity infrastructure often lags. This study evaluates cybersecurity infrastructure in selected HEIs in Delta State, Nigeria, with a focus on technology availability, policy effectiveness, user awareness, and implementation challenges. A survey of 387 stakeholders, including IT personnel, academic and administrative staff, and students, yielded a 100% response rate, with data analyzed using descriptive statistics and a 3.50 mean threshold on a 5-point Likert scale. Results indicate broad use of basic protective tools like firewalls and antivirus software, contrasted by sparse deployment of advanced systems such as intrusion detection and security monitoring platforms. While formal policies are generally present, their enforcement, auditing processes, and incident response mechanisms prove inconsistent and underdeveloped. Threat awareness exists at a moderate level among users, yet formal training and institutional programs remain inadequate. Primary obstacles encompass chronic funding deficits, subpar ICT foundations, and shortages of skilled personnel. These institutions display incomplete cybersecurity maturity, heightening risks within their open-access networks and remote learning setups. Proposed actions urge prioritizing advanced technologies, strengthening policy execution through specialized units, rolling out mandatory awareness initiatives, securing greater financial support for capacity building and operations centers, and promoting partnerships to exchange threat insights. Such steps promise to bolster institutional defenses and support national goals for secure digital education environments.

Keywords: Higher Education Institutions, cybersecurity, Information Technology, phishing, Malware.

Introduction

The rapid digital transformation of Higher Education Institutions (HEIs) has fundamentally reshaped academic delivery, research processes, and administrative operations. Universities now depend heavily on digital infrastructures such as cloud computing, learning management systems, and interconnected research platforms, which enhance efficiency and global collaboration. However, this transformation has also increased exposure to cyber threats, including ransomware, phishing, data breaches, and insider attacks (Afolalu & Tsoeu, 2025; Chapman, 2019). Cybersecurity infrastructure in HEIs, therefore, represents an integrated system of technologies, policies, governance frameworks, and human competencies designed to safeguard institutional data and ensure the confidentiality, integrity, and availability of information systems (Singar and Akhilesh, 2019; Cheng & Wang, 2022).

A key characteristic of HEIs is their open-access environment, which promotes knowledge sharing and academic freedom but simultaneously creates significant security vulnerabilities. Unlike corporate organizations with controlled systems, universities often allow broad access to networks for students, staff, and external collaborators, thereby increasing their attack surface and complicating cybersecurity enforcement (Cojocariu et al., 2019; Maranga & Nelson, 2019). This challenge has been further intensified by the rise of remote learning and digital platforms, especially following global disruptions such as the COVID-19 pandemic, which expanded reliance on virtual environments and heightened exposure to cyber risks (Alexei & Alexei, 2021).

The cybersecurity threat landscape in HEIs continues to evolve, with institutions increasingly targeted due to the high value of their data assets, including intellectual property, research findings, and personal information (Binitie et al., 2025; Fouad, 2021). These threats stem from both external actors and internal vulnerabilities such as weak authentication systems, outdated software, and inadequate monitoring mechanisms (Kryshtanovych et al., 2021; Ganesen et al., 2022). As a result, higher education institutions have become one of the most targeted sectors globally, largely due to their decentralized IT environments and relatively weaker security structures (Afolalu & Tsoeu, 2025).

Effective cybersecurity infrastructure in HEIs comprises interconnected components, including technological systems (for instance, firewalls, intrusion detection systems, encryption, and SIEM tools), policy and governance frameworks, human awareness, and continuous risk assessment processes (Nassoura, 2022; Yusif & Hafeez-Baig, 2023; Haque et al., 2023). These components must operate cohesively to

ensure resilience. Institutional strategies such as leadership commitment, proactive risk management, incident response planning, and continuous monitoring are also essential for strengthening cybersecurity (Cheng & Wang, 2022; Alexei, 2021). Additionally, cybersecurity is increasingly viewed not only as an institutional issue but as a broader national concern due to the strategic role of universities in innovation and knowledge production (Fouad, 2021).

Despite growing awareness, HEIs face persistent challenges, including inadequate funding, a shortage of skilled personnel, decentralized systems, weak policy enforcement, and insufficient cybersecurity education (Mogoane & Kabanda, 2019; Maranga & Nelson, 2019; Catota et al., 2019). While existing literature provides valuable insights into these issues, most studies focus on isolated aspects such as technology or policy, with limited integration of human and organizational factors. Furthermore, there is a lack of context-specific empirical research in developing countries like Nigeria. This study addresses these gaps by providing a comprehensive empirical assessment of cybersecurity infrastructure in HEIs, examining its components, effectiveness, and challenges within a unified framework.

Problem statement

The rapid digital transformation of Higher Education Institutions (HEIs) has significantly increased their exposure to cyber threats, yet the development of robust cybersecurity infrastructure has not kept pace with this expansion. Universities manage vast volumes of sensitive data, including academic records, research outputs, and financial information, making them prime targets for cyberattacks (Fouad, 2021; Chapman, 2019). However, many HEIs still rely on basic security measures, with limited adoption of advanced technologies such as intrusion detection systems and security information and event management tools (Nassoura, 2022), while cybersecurity governance remains fragmented due to decentralized IT structures and weak policy enforcement (Maranga & Nelson, 2019; Cheng & Wang, 2022). Compounding this challenge is the low level of cybersecurity awareness among users, which increases vulnerability to attacks such as phishing and credential theft (Yusif & Hafeez-Baig, 2023; Catota et al., 2019), alongside the expanded risks introduced by remote learning and the use of unsecured personal devices (Alexei & Alexei, 2021). In developing contexts such as Nigeria, these issues are further exacerbated by limited funding, inadequate skilled personnel, and weak institutional frameworks (Mogoane & Kabanda, 2019; Ganesen et al., 2022). Despite existing studies, there remains a lack of comprehensive empirical research that integrates technological, organizational, and human factors in assessing cybersecurity infrastructure in HEIs, thereby creating a critical gap in understanding how to enhance institutional cybersecurity resilience effectively.

Purpose of the Study

The main purpose of the study was to evaluate the state of cybersecurity infrastructure in Higher Education Institutions (HEIs). Specifically, the study sought to:

1. examine the availability of cybersecurity technologies and infrastructures in Higher Education Institutions.
2. assess the effectiveness of cybersecurity policies, governance structures, and institutional strategies.
3. evaluate the level of cybersecurity awareness and compliance among students and staff in HEIs.
4. identify the major challenges affecting the implementation of cybersecurity infrastructure in HEIs.

Research Questions

The study is guided by the following research questions:

1. What cybersecurity technologies and infrastructure are available in Higher Education Institutions?
2. How effective are cybersecurity policies, governance structures, and institutional strategies in HEIs?
3. What is the level of cybersecurity awareness and compliance among students and staff in HEIs?
4. *What are the major challenges affecting the implementation of cybersecurity infrastructure in Higher Education Institutions?*

Research Design

The research design adopted for the study is survey design.

Area of the Study

The study is conducted in selected Higher Education Institutions in Delta State, Nigeria. The focus on this area is informed by the increasing adoption of digital technologies in universities within the state and the need to evaluate their preparedness against cyber threats. Institutions considered include federal, state, and private universities to ensure a comprehensive representation of the higher education landscape.

Population of the Study

The population of the study comprises all relevant stakeholders within the selected Higher Education Institutions, including Information Technology (IT) personnel, Academic staff, administrative staff, and Students.

Sample Size and Sampling Technique

The study targeted key stakeholders within selected Higher Education Institutions in Delta state in Nigeria, including Information Technology (IT) personnel, academic staff, administrative staff, and students. A total of 387 respondents participated in the study, providing insights into the availability, effectiveness, challenges, and overall state of

cybersecurity infrastructure within their institutions. A combination of stratified and purposive sampling techniques was employed to select participants. Stratified sampling ensured that all relevant groups within the institutions were adequately represented, while purposive sampling was used to specifically select respondents with relevant knowledge or experience in the use, management, or interaction with institutional information systems. This approach was appropriate given the multi-dimensional nature of cybersecurity infrastructure, which requires input from both technical experts and general users. Additionally, elements of convenience sampling were applied in reaching accessible respondents within each stratum, thereby enhancing participation rates. Before full deployment, the questionnaire was pre-tested with a small group of respondents outside the study sample to ensure clarity, validity, and reliability of the instrument. Ethical standards were strictly upheld through informed consent, voluntary participation, anonymity, and confidentiality, with no personally identifiable information collected from participants.

Method of Data Collection

Data for this study were collected using a structured questionnaire titled "Cybersecurity Infrastructure Evaluation Questionnaire (CIEQ)". The instrument was designed to obtain quantitative data on the availability of cybersecurity technologies, the effectiveness of institutional policies and governance frameworks, and the level of cybersecurity awareness among respondents in Higher Education Institutions (HEIs).

The questionnaire consisted of five sections: Section one covers the respondent's demographic information, while the other four sections cover the research questions.

The instrument adopted a 5-point Likert scale ranging from Strongly Agree (5), Agree (4), Neutral (3), Disagree (2), Strongly Disagree (1) to measure respondents' perceptions. Data collection was carried out through both online (Google Forms) and physical administration of questionnaires to ensure wider coverage and improved response rate. Respondents were given adequate time to complete the questionnaire, and follow-ups were conducted to maximize retrieval. Of the 387 questionnaires distributed, all were completed and returned, yielding a 100% response rate for analysis.

Results presentation

This section reports the empirical results of the study, based on responses from 387 respondents. Descriptive statistics, such as mean scores and standard deviations, were employed to analyze the data in relation to the research questions. Responses in Table 1 were captured in percentages, while responses from Tables 2 through 4 were captured using a five-point Likert scale. A threshold mean score of 3.50 was set to differentiate between accepted and rejected items, so that only items with a clear lean toward agreement were treated as significant. Items with a mean value of 3.50 and above were regarded as accepted, while those with a mean value less than 3.50 were regarded as rejected.

Research Question 1: What cybersecurity technologies and infrastructure are available in Higher Education Institutions?

Table 1 presents the percentage of availability of cybersecurity infrastructure in HEIs.

Table 1: Availability of Cybersecurity Infrastructure (n = 387)

S/N	Cybersecurity Infrastructure	Available (Freq.)	Available (%)	Not Available (Freq.)	Not Available (%)
1	Firewalls	329	85.0%	58	15.0%
2	Antivirus Software	302	78.0%	85	22.0%
3	Multi-Factor Authentication	201	52.0%	186	48.0%
4	Intrusion Detection Systems	159	41.1%	228	58.9%
5	Data Encryption Systems	174	45.0%	213	55.0%
6	SIEM Systems	116	30.0%	271	70.0%

Source: Field work (2026)

The results in Table 1 show that basic cybersecurity technologies, such as firewalls (85.0%) and antivirus software (78.0%), are widely available across institutions, indicating strong adoption. However, more advanced systems, such as intrusion detection systems (41.1%), data encryption systems (45.0%), and SIEM systems (30.0%), have considerably lower availability. This indicates that while foundational cybersecurity tools are largely in place, the adoption of advanced infrastructure for proactive threat detection and monitoring is limited and unevenly distributed across institutions

Research Question 2: How effective are cybersecurity policies, governance structures, and institutional strategies in HEIs?

Table 2 presents respondents' perceptions of the effectiveness of cybersecurity policies and governance.

Table 2: Effectiveness of Cybersecurity Policies and Governance (n = 387)

S/N	Statement	SA	A	N	D	SD	Mean	Std. Dev
1	Clear cybersecurity policy exists	102	118	76	61	30	3.52	1.01
2	Policies are effectively enforced	85	110	80	72	40	3.33	1.08
3	Dedicated cybersecurity unit exists	95	104	60	78	50	3.30	1.12
4	Regular security audits are conducted	70	98	90	85	44	3.17	1.09
5	Incident response plans are established	68	95	88	86	50	3.11	1.13

Source: Field work (2026)

Table 2 shows that cybersecurity policies and governance structures are moderately effective. The presence of clear policies (Mean = 3.52, SD = 1.01) slightly exceeds the acceptance threshold, indicating general agreement among respondents. However, enforcement (Mean = 3.33, SD = 1.08), existence of dedicated units (Mean = 3.30, SD = 1.12), security audits (Mean = 3.17, SD = 1.09), and incident response plans (Mean = 3.11, SD = 1.13) fall below the threshold, suggesting weak implementation. The relatively higher standard deviations indicate

variability in institutional practices, implying inconsistency in policy execution across HEIs. This reflects a governance structure that exists in principle but is not uniformly operationalized.

Research Question 3: What is the level of cybersecurity awareness and compliance among students and staff in HEIs?

Table 3 presents responses on cybersecurity awareness and practices

Table 3: Cybersecurity Awareness and Practices (n = 387)

S/N	Statement	SA	A	N	D	SD	Mean	Std. Dev
1	Awareness of cyber threats	110	120	70	60	27	3.59	0.98
2	Strong password practices	98	115	75	65	34	3.46	1.05
3	Received cybersecurity training	65	90	80	95	57	3.03	1.14
4	Ability to identify phishing	80	102	78	85	42	3.24	1.10
5	Institution conducts awareness programs	60	85	90	95	57	2.98	1.16

Source: Field work (2026)

The results in Table 3 indicate a moderate level of cybersecurity awareness. Awareness of cyber threats (Mean = 3.59, SD = 0.98) is relatively high with low variability, indicating consistent knowledge among respondents. However, training (Mean = 3.03, SD = 1.14) and institutional awareness programs (Mean = 2.98, SD = 1.16) are low, with higher standard deviations suggesting uneven exposure across respondents. This implies that awareness is largely informal and not systematically developed through institutional efforts, leaving users vulnerable to cyber threats.

Research question 4: What are the major challenges affecting the implementation of cybersecurity infrastructure in HEIs?

Table 4 presents the major challenges affecting cybersecurity implementation.

Table 4: Challenges Affecting Cybersecurity Implementation (n = 387)

S/N	Challenge Items	SA	A	N	D	SD	Mean	Std. Dev
1	Inadequate funding	150	132	60	30	15	3.90	0.89
2	Lack of skilled professionals	120	140	65	40	22	3.66	0.95
3	Weak cybersecurity policies	110	125	70	50	32	3.47	1.02
4	Poor ICT infrastructure	135	130	55	40	27	3.73	0.91
5	Low user awareness	105	120	80	55	27	3.42	1.04
6	Weak policy enforcement	115	130	70	45	27	3.55	0.98

Table 4 shows that inadequate funding (Mean = 3.90, SD = 0.89) is the most significant challenge, with strong agreement and low variability among respondents. Poor ICT infrastructure (Mean = 3.73, SD = 0.91) and lack of skilled professionals (Mean = 3.66, SD = 0.95) are also major constraints. Weak policy enforcement (Mean = 3.55, SD = 0.98) slightly exceeds the threshold, indicating it is a notable concern. Meanwhile, weak policies (Mean =

3.47, SD = 1.02) and low awareness (Mean = 3.42, SD = 1.04) fall below the threshold, though their relatively high standard deviations suggest variability across institutions. Overall, the results indicate that cybersecurity challenges in HEIs are multidimensional, involving financial, technical, and human factors.

Discussion of Results

The findings of this study reveal the current state of cybersecurity infrastructure in Higher Education Institutions (HEIs), highlighting the extent of technological deployment, the effectiveness of institutional policies, and the level of cybersecurity awareness among users. Respondents indicated across all research questions that foundational cybersecurity systems are widely present, while significant gaps persist in advanced technological adoption, policy enforcement, and structured awareness programs.

Regarding the availability of cybersecurity infrastructure, respondents reported high deployment of basic tools such as firewalls and antivirus systems, while more advanced systems such as intrusion detection systems, encryption frameworks, and Security Information and Event Management (SIEM) systems were significantly underutilized. This suggests that HEIs have achieved only partial digital security maturity, relying heavily on preventive rather than predictive or proactive cybersecurity technologies. This finding aligns with Nassoura (2022) and Afolalu and Tsoeu (2025), who observed that many higher education institutions globally still depend on conventional security tools due to financial limitations, lack of expertise, and infrastructural constraints. Similarly, Chapman (2019) emphasized that although universities are increasingly digitized, their cybersecurity preparedness often lags behind their technological adoption, creating critical vulnerability gaps.

On cybersecurity policies and governance structures, the results indicate a moderate level of effectiveness. While many institutions reportedly have formal cybersecurity policies and dedicated units, enforcement and implementation remain inconsistent. Respondents expressed concerns about weak incident response systems, limited security audits, and inadequate institutional coordination. This finding supports Cheng and Wang (2022), who argued that cybersecurity effectiveness in HEIs depends not only on policy existence but also on enforcement mechanisms and leadership commitment. Likewise, Alexei (2021) noted that many institutions adopt cybersecurity strategies in principle but fail to operationalize them effectively due to governance fragmentation and insufficient monitoring systems. The implication is that cybersecurity governance in HEIs remains largely reactive rather than proactive.

The study further revealed a moderate level of cybersecurity awareness and compliance among students and staff. While respondents demonstrated awareness of common cyber threats such as phishing and malware, participation in formal cybersecurity training programs and institutional awareness initiatives was relatively low. This suggests that cybersecurity knowledge is largely informal and user-driven rather than institutionally structured. This finding is consistent with Catota et al. (2019), who emphasized that cybersecurity education

in HEIs, particularly in developing contexts, remains underdeveloped and unevenly distributed. Yusif and Hafeez-Baig (2023) also highlighted that weak cybersecurity compliance is often linked to inadequate awareness programs and limited behavioral reinforcement mechanisms within institutions.

Furthermore, the results reflect broader systemic challenges affecting cybersecurity infrastructure in HEIs, including inadequate funding, a shortage of skilled cybersecurity professionals, and a lack of continuous capacity development. These challenges are consistent with the observations of Mogoane & Kabanda (2019) and Ganesen et al. (2022), who identified resource constraints and institutional inefficiencies as major barriers to effective cybersecurity implementation in higher education settings. Additionally, Alexei and Alexei (2021) noted that the expansion of remote learning environments has further exposed institutional weaknesses, increasing the attack surface and complicating security enforcement.

The findings demonstrate that although HEIs have made progress in adopting basic cybersecurity technologies and establishing formal policies, their overall cybersecurity infrastructure remains underdeveloped and unevenly implemented. The results align with Fouad (2021), who argued that cybersecurity in higher education should be viewed as both an institutional and national priority due to its implications for data protection, research integrity, and digital trust. The study therefore reinforces the broader literature, which suggests that effective cybersecurity in HEIs requires an integrated approach combining technological advancement, strong governance frameworks, and sustained human capacity development (Kryshtanovych et al., 2021; Cheng & Wang, 2022; Afolalu & Tsoeu, 2025).

Conclusion

This study examined cybersecurity infrastructure in Higher Education Institutions (HEIs) with a focus on the availability of technological systems, the effectiveness of institutional policies and governance, and the level of cybersecurity awareness among users. The findings reveal that while HEIs have adopted basic cybersecurity technologies such as firewalls and antivirus systems, the deployment of advanced security solutions such as intrusion detection systems, encryption frameworks, and Security Information and Event Management (SIEM) systems remains limited. Furthermore, although most institutions have established formal cybersecurity policies, their implementation and enforcement are inconsistent, reflecting weaknesses in governance structures and institutional coordination. The study also established that cybersecurity awareness among students and staff is moderate, with limited access to structured training and awareness programs. Overall, the study concludes that cybersecurity infrastructure in HEIs is still developing and insufficient to effectively counter the growing sophistication of cyber threats, thereby exposing institutions to significant operational and data security risks.

Recommendations

Based on the findings of the study, the following recommendations are made:

1. Higher Education Institutions should invest in advanced cybersecurity tools such as intrusion detection systems (IDS), Security Information and Event Management (SIEM) systems, artificial intelligence-based threat detection, and robust encryption mechanisms to enhance proactive threat prevention and response capabilities.
2. Institutions should develop clear, enforceable, and regularly updated cybersecurity policies. Dedicated cybersecurity units should be empowered with the authority and resources to ensure strict compliance and continuous monitoring of institutional systems.
3. HEIs should implement compulsory cybersecurity awareness programs for students, academic staff, and administrative personnel. Continuous training should be introduced to improve users' ability to identify and respond to cyber threats such as phishing and malware attacks.
4. Governments and institutional management should allocate adequate financial resources to cybersecurity development, including infrastructure upgrades, staff training, and recruitment of skilled cybersecurity professionals.
5. Universities should establish fully functional Security Operations Centers (SOCs) and incident response frameworks to enable real-time monitoring, detection, and mitigation of cyber threats.
6. HEIs should collaborate with cybersecurity agencies, industry experts, and other institutions to share threat intelligence, best practices, and emerging security solutions.

References

Afolalu, O., & Tsoeu, M. S. (2025). Cybersecurity in higher education institutions: A systematic review of emerging trends, challenges, and solutions. *Future Internet, 17*(12), 575.

Alexei, L. A. (2021). Cybersecurity strategies for higher education institutions. *Journal of Engineering Science*, (4), 74–92.

Alexei, L. A., & Alexei, A. (2021). Cybersecurity threat analysis in higher education institutions as a result of distance learning. *International Journal of Scientific and Technology Research, 10*(3), 128–133.

Binitie, A. P., Onyemene, I. S., & Okoh, J. F. (2025). Enhancing security and privacy in edtech tools: safeguarding student data in the digital learning era. *Journal of Science Innovation and Technology Research, 9(9),* 27-36.

Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. *Journal of Cybersecurity, 5*(1), tyz001. https://doi.org/10.1093/cybsec/tyz001

Chapman, J. (2019). *How safe is your data? Cyber-security in higher education* (HEPI Report No. 12). Higher Education Policy Institute.

Cheng, E. C., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. *Information, 13*(4), 192. https://doi.org/10.3390/info13040192

Cojocariu, A. C., Verzea, I., & Chaib, R. (2019). Aspects of cyber-security in higher education institutions. In *International Symposium in Management Innovation for Sustainable Management and Entrepreneurship* (pp. 3–11). Springer.

Fouad, N. S. (2021). Securing higher education against cyberthreats: From an institutional risk to a national policy challenge. *Journal of Cyber Policy, 6*(2), 137–154. https://doi.org/10.1080/23738871.2021.1934662

Ganesen, R., Bakar, A. A., Ramli, R., Rahim, F. A., & Zawawi, M. N. A. (2022). Cybersecurity risk assessment: Modeling factors associated with higher education institutions. *International Journal of Advanced Computer Science and Applications, 13*(8).

Haque, M. A., Ahmad, S., John, A., Mishra, K., Mishra, B. K., Kumar, K., & Nazeer, J. (2023). Cybersecurity in universities: An evaluation model. *SN Computer Science*, *4*(5), 569.

Kryshtanovych, M., Kozlovskiy, Y., Chubinska, N., Huzii, I., & Lukashevska, U. (2021). Ensuring cybersecurity for higher educational institutions. In *2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)* (pp. 183–186). IEEE.

Maranga, M. J., & Nelson, M. (2019). Emerging issues in cybersecurity for institutions of higher education. *International Journal of Computer Science and Network, 8*(4), 371–379.

Mogoane, S. N., & Kabanda, S. (2019). Challenges in information and cybersecurity program offering at higher education institutions. In *ICICIS* (pp. 202–212).

Nassoura, A. B. (2022). Cybersecurity technologies and practices in higher education institutions: A systematic review. *Webology, 19*(3).

Singar, A. V., & Akhilesh, K. B. (2019). Role of cyber-security in higher education. In *Smart Technologies: Scope and Applications* (pp. 249–264). Springer.

Yusif, S., & Hafeez-Baig, A. (2023). Cybersecurity policy compliance in higher education: A theoretical framework. *Journal of Applied Security Research, 18*(2), 267–288. https://doi.org/10.1080/19361610.2022.2065367