OPEN ACCESS

Journal of Advances in Education and Philosophy

Abbreviated Key Title: J Adv Educ Philos
ISSN 2523-2665 (Print) |ISSN 2523-2223 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://saudijournals.com

Original Research Article

Evaluating the Effectiveness of Cybersecurity Measures in Safeguarding Online Educational Resources: A Case Study of the University of Port Harcourt Open and Distance Learning System

Dr. Abe Ezinne Chidinma[1*], Adoghe Jessy-Harrison Idemudia[2]

[1]University of Portharcourt, Faculty of Education, Department of Curriculum Studies and Educational Technology. Uniport. Rivers State, Nigeria
[2]National Open University of Nigeria, (Port Harcourt Study Center), Department of Educational Technology, Faculty of Education, Port Harcourt. Rivers State, Nigeria

DOI: https://doi.org/10.36348/jaep.2025.v09i07.003 | **Received:** 02.06.2025 | **Accepted:** 17.07.2025 | **Published:** 28.07.2025

***Corresponding author:** Dr. Abe Ezinne Chidinma
University of Portharcourt, Faculty of Education, Department of Curriculum Studies and Educational Technology. Uniport. Rivers State, Nigeria

Abstract

As the digitization of education intensifies, cybersecurity has become a vital concern, particularly for Open and Distance Learning (ODL) systems that rely heavily on online platforms to deliver instructional content and manage academic resources. This study investigates the effectiveness of cybersecurity measures implemented within the University of Port Harcourt's ODL system, with a focus on protecting online educational resources. The research further examines specific vulnerabilities and challenges affecting the cybersecurity infrastructure, such as user awareness, policy implementation, and technical capacity. Adopting a quantitative research approach, data were collected via structured questionnaires distributed to ODL users, and analyzed using descriptive statistics, specifically the mean. The findings indicate that while users express moderate confidence in the presence of basic cybersecurity measures, they also highlight critical shortcomings, including insufficient training, unclear security policies, and irregular system audits. These deficiencies pose significant risks to the safety and integrity of online educational resources. Based on these findings, the study concludes that although foundational security measures exist, a lack of strategic coordination and user engagement weakens overall cybersecurity effectiveness. Consequently, recommendations are made for institutional actors to prioritize awareness training, policy dissemination, continuous audits, and resource allocation to strengthen the ODL platform's security posture.

Keywords: Cybersecurity, Open and Distance Learning (ODL), Online Educational Resources, Vulnerabilities, User Awareness.

INTRODUCTION

The digital transformation of education has significantly reshaped the global academic landscape, enabling institutions to adopt innovative learning modalities such as Open and Distance Learning (ODL). With the emergence of online educational platforms, universities are increasingly relying on digital infrastructures to facilitate learning, communication, assessment, and resource management. The University of Port Harcourt (UNIPORT), like many other higher institutions, has embraced this transformation through the implementation of an ODL system aimed at providing flexible access to education. This system is instrumental in catering to a diverse and geographically dispersed student population, thereby aligning with global trends towards inclusive and technology-driven education (UNESCO, 2020).

However, the increased reliance on digital platforms has introduced significant cybersecurity concerns. As online educational resources become more integral to teaching and learning, they simultaneously become attractive targets for cyber threats such as unauthorized access, data breaches, denial-of-service attacks, and the manipulation of digital content. These threats have the potential to undermine the integrity, confidentiality, and availability of educational data, posing substantial risks to institutional credibility and the academic welfare of students and staff (Alotaibi, 2020).

Given the sensitive nature of student records, assessment data, and intellectual property, safeguarding these resources has become a strategic imperative for universities across the globe.

In the context of Nigeria's educational sector, cybersecurity remains a relatively underexplored and underfunded domain, despite the growing prevalence of cyber-related incidents. Studies have shown that many Nigerian institutions lack the robust cybersecurity frameworks necessary to counteract sophisticated cyber threats effectively (Adebesin & Shange, 2021). Furthermore, limited technical capacity, policy implementation gaps, and inadequate awareness among users often exacerbate vulnerabilities within these systems. The University of Port Harcourt's ODL system, being heavily reliant on web-based interfaces and digital resource management tools, is not immune to these challenges. Therefore, an empirical evaluation of the effectiveness of existing cybersecurity measures in protecting these systems is both timely and necessary.

Assessing cybersecurity effectiveness in educational systems involves a multifaceted approach that considers technical safeguards, administrative policies, user awareness, and incident response mechanisms. A number of frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and ISO/IEC 27001, have been developed to guide institutions in implementing comprehensive cybersecurity strategies (NIST, 2020). However, the contextual application of these frameworks within the Nigerian educational setting, particularly at UNIPORT, warrants localized investigations to account for infrastructural, financial, and socio-technical dynamics. This paper seeks to fill a critical gap in the literature by conducting a case-specific analysis of UNIPORT's ODL cybersecurity posture.

Statement of Problem

The rapid integration of digital technologies in higher education has revolutionized teaching and learning, particularly through Open and Distance Learning (ODL) systems. At the University of Port Harcourt, the adoption of an ODL platform has opened new educational opportunities for a diverse range of learners. However, this technological advancement has also brought with it a host of cybersecurity vulnerabilities that threaten the confidentiality, integrity, and availability of online educational resources. Despite the centrality of these resources to academic success, there is growing concern that the existing cybersecurity measures implemented within the University's ODL system may be insufficient or inconsistently applied.

Preliminary observations and emerging literature suggest that Nigerian higher education institutions, including UNIPORT, often face significant challenges in implementing effective cybersecurity frameworks. These challenges stem from limited technical capacity, lack of comprehensive cybersecurity policies, low levels of user awareness, and inadequate resource allocation (Adebesin & Shange, 2021; Alotaibi, 2020). Consequently, systems meant to support learning are becoming increasingly susceptible to cyber threats such as unauthorized data access, system intrusions, phishing attacks, and the manipulation of sensitive academic records. These issues not only compromise institutional data security but also risk eroding stakeholder trust in digital education.

Despite the critical role of cybersecurity in ensuring the reliability and sustainability of ODL platforms, there is a conspicuous gap in empirical investigations focused on evaluating the actual effectiveness of these protective measures within Nigerian universities. Specifically, there is a lack of localized evidence that assesses how well these cybersecurity controls function in practice within the University of Port Harcourt's ODL system. Without a systematic evaluation, it remains unclear whether current measures are sufficient, where vulnerabilities lie, and what strategies can be improved to better safeguard the institution's digital learning infrastructure. This gap necessitates a focused empirical inquiry into the effectiveness of cybersecurity measures employed in the University of Port Harcourt's ODL system.

OBJECTIVES

The following objectives were formulated for this paper:

1. To evaluate the effectiveness of existing cybersecurity measures implemented within the University of Port Harcourt's Open and Distance Learning (ODL) system in protecting online educational resources.
2. To identify specific vulnerabilities and challenges affecting the cybersecurity infrastructure of the University's ODL platform, including user awareness, policy implementation, and technical controls.
3. To propose strategic improvements and best practices for enhancing the cybersecurity framework of the University of Port Harcourt's ODL system based on empirical findings.

LITERATURE REVIEW

Cybersecurity in Higher Education

The increasing digitization of academic services and resources has made cybersecurity a pressing concern for institutions of higher learning. Universities around the world have adopted digital infrastructures to support teaching, research, student administration, and communication. However, this transformation has significantly expanded the cybersecurity threat surface. Higher education institutions are now key targets for cybercriminals due to their vast repositories of sensitive information, including student records, intellectual property, research data, and financial details (Alasmary *et al.,* 2022). The decentralized nature of university

networks, coupled with their openness to a wide variety of users—students, staff, researchers, and external partners—makes them particularly vulnerable to attacks such as phishing, ransomware, identity theft, and unauthorized data access.

Cybersecurity in higher education is further complicated by the diversity of digital platforms and devices that users bring to the network environment. With the rise of bring-your-own-device (BYOD) policies, online learning platforms, cloud storage, and third-party educational applications, institutions are required to manage an increasingly complex digital ecosystem (Patil & Patil, 2020). As a result, universities must adopt robust security frameworks that ensure the confidentiality, integrity, and availability of digital resources. These frameworks often include technical controls such as firewalls, intrusion detection systems, encryption protocols, and endpoint protection tools. However, technical solutions alone are not sufficient; cybersecurity also requires strong administrative policies, user education, and continuous monitoring and response capabilities (Hewitt *et al.,* 2021).

In many cases, the challenge lies not in the absence of cybersecurity policies, but in the lack of proper implementation and enforcement. Universities may develop comprehensive security policies, yet struggle to communicate and operationalize them effectively across various departments and user groups. Faculty and students often lack awareness of basic cybersecurity practices, making them easy targets for social engineering attacks. For example, phishing remains one of the most common and successful attack vectors in educational settings, largely because users are not adequately trained to recognize suspicious emails or links (Susanto & Almunawar, 2020). Moreover, the academic culture of openness and information sharing, while essential to learning and innovation, can conflict with the principles of restrictive cybersecurity.

In developing countries, the cybersecurity challenges faced by higher education institutions are even more pronounced due to limited funding, inadequate infrastructure, and insufficient policy support. Many universities struggle to keep up with the rapid evolution of cyber threats, as they lack both the financial resources to invest in advanced security technologies and the skilled personnel to manage them (Adebayo & Kehinde, 2022). In Nigeria, for instance, the growing use of online learning systems has exposed universities to a range of digital threats, yet cybersecurity governance remains weak. Institutions often rely on outdated software, lack centralized IT oversight, and provide minimal training to system users.

The COVID-19 pandemic significantly accelerated the shift to online learning, further highlighting the cybersecurity deficiencies in higher education. As universities rapidly transitioned to remote instruction, many were unprepared to secure their digital platforms effectively. This led to increased instances of cyberattacks, including Zoom-bombing, data leaks, and denial-of-service attacks (Cheng & Jin, 2021). These incidents underscored the urgent need for higher education institutions to prioritize cybersecurity as a strategic objective rather than a purely technical concern.

Addressing cybersecurity in higher education requires a multi-layered approach that combines technological tools, institutional policies, and user behavior management. Institutions must also build a culture of cybersecurity awareness, where all stakeholders understand their role in protecting digital assets. International standards such as the ISO/IEC 27001 and the NIST Cybersecurity Framework can serve as valuable guides in developing institutional security policies. However, these frameworks must be adapted to local contexts, taking into account the institution's size, digital maturity, and risk environment (Alshaikh, 2020).

Open and Distance Learning (ODL) Systems

Open and Distance Learning (ODL) systems have emerged as a transformative approach to delivering education, particularly in addressing issues of access, flexibility, and scalability. Unlike traditional classroom-based learning, ODL allows students to learn remotely through digital platforms, printed materials, or broadcast media, without the need for physical presence in a conventional educational setting. This model of learning has gained significant traction globally, especially in response to the rising demand for higher education and the need to accommodate diverse learner populations, including working adults, rural dwellers, and individuals with disabilities (Kirkwood & Price, 2021). The promise of open access, self-paced learning, and broader participation makes ODL a strategic response to educational inequalities, particularly in developing countries where institutional capacity may be limited.

Technological advancements have played a critical role in shaping modern ODL systems. The proliferation of the internet, smartphones, learning management systems (LMS), and digital content has enabled educational institutions to deliver instructional materials in multimedia formats, host real-time virtual classes, and assess learners through interactive online platforms. According to Al-Fraihat *et al*. (2020), the success of ODL depends not only on the availability of content but also on the quality of learner support, user-friendly interfaces, and consistent access to technological infrastructure. Learning platforms like Moodle, Blackboard, and Canvas are now widely used to host course content, discussions, quizzes, and other instructional resources. These systems are essential in enabling effective asynchronous and synchronous learning experiences.

In the context of Sub-Saharan Africa, including Nigeria, ODL offers immense potential to bridge the

educational gap. The University of Port Harcourt, like many other institutions, has adopted ODL to expand its academic reach and reduce the infrastructural burden associated with in-person education. However, challenges remain. The effectiveness of ODL in Nigeria is often hampered by inadequate internet penetration, erratic power supply, limited digital literacy among users, and institutional underfunding (Adedoyin & Soykan, 2020). These constraints affect both students and academic staff, making it difficult to fully realize the benefits of digital education. In addition, the lack of locally relevant digital content and support systems can create disconnects between technology and pedagogy.

Another significant concern with ODL systems is the issue of academic integrity and the quality of learning outcomes. The remote nature of ODL can sometimes create opportunities for academic dishonesty, such as impersonation, plagiarism, and cheating during assessments. To counter these threats, institutions are increasingly turning to proctoring software, plagiarism detection tools, and biometric verification systems (Dhawan, 2020). However, the integration of such security mechanisms raises additional concerns about data privacy, digital rights, and student surveillance. Therefore, managing ODL systems requires a delicate balance between technological innovation and ethical considerations.

The COVID-19 pandemic served as a major turning point for ODL globally. During the crisis, institutions were forced to shift to remote teaching almost overnight, accelerating the adoption of ODL methodologies. While this transition was more seamless in developed nations with robust digital infrastructures, many institutions in developing countries faced serious challenges. Nevertheless, the pandemic highlighted the importance of building resilient educational systems that can withstand disruptions and continue to deliver quality education through digital means (Mseleku, 2020). For the University of Port Harcourt and similar institutions, this period underscored the urgent need to invest in ODL platforms, improve cybersecurity, and train stakeholders on the use of digital tools for teaching and learning.

Cyber Threats and Vulnerabilities in Online Education

As education continues to shift toward digital platforms, the exposure of online learning environments to cyber threats has grown significantly. Online education systems, particularly those used in higher institutions, have become attractive targets for cybercriminals due to the massive amount of sensitive data they house, including personal information of students and staff, academic records, financial details, and proprietary research. The vulnerabilities in these systems arise from various sources, including technological weaknesses, human error, inadequate policies, and a general lack of cybersecurity awareness. According to Alharthi *et al*. (2020), one of the biggest challenges is that many educational institutions are not fully prepared to identify or respond to cyber threats in a timely and effective manner.

A major type of threat faced by online education platforms is phishing—fraudulent attempts to gain access to user credentials or sensitive information through deceptive emails or messages. Educational users, including students and faculty, often lack formal training in cybersecurity, making them vulnerable to these schemes. Phishing attacks may lead to data breaches, unauthorized access to institutional systems, or identity theft. Another common threat is ransomware, a type of malware that encrypts data and demands payment for its release. In several documented cases, universities around the world have been forced to suspend operations due to ransomware attacks, resulting in severe disruptions to academic services (Johnson *et al.,* 2021). These incidents highlight the urgent need for educational institutions to implement comprehensive threat detection and response strategies.

Aside from external attacks, internal vulnerabilities also pose significant risks to online education. Insider threats—whether intentional or accidental—can lead to data loss or security breaches. This may involve students sharing login credentials, staff mishandling data, or administrators using weak passwords. Misconfigurations in learning management systems (LMS), failure to install software updates, and reliance on outdated technology further increase institutional exposure to cyber threats. According to Fikri and Setiawan (2021), many online education platforms suffer from insufficient access controls and poorly enforced authentication mechanisms, which make it easier for unauthorized users to infiltrate systems.

The rapid growth in the use of third-party tools and software in online education has also contributed to the rising cybersecurity risks. Applications like Zoom, Google Meet, and collaborative platforms such as Slack or Microsoft Teams became widely adopted during the COVID-19 pandemic, but many were initially not designed with education-specific security needs in mind. A notable example is "Zoom-bombing"—the unwanted intrusion into video conferencing sessions—which disrupted thousands of online classes globally in 2020. These incidents revealed critical flaws in the default privacy settings of such platforms and emphasized the need for institutions to conduct thorough security assessments before integrating third-party technologies into their learning environments (Salloum *et al.,* 2021).

In the developing world, including Nigeria, the threats to online education systems are exacerbated by infrastructural and resource constraints. Institutions may not have the capacity to employ dedicated cybersecurity personnel or afford advanced security solutions. Moreover, awareness campaigns and cybersecurity training programs are either underfunded or nonexistent. This leaves many students and educators ill-equipped to

protect themselves in digital spaces. As Osuagwu and Chukwudebe (2022) observed, there is a low level of cybersecurity literacy among Nigerian university communities, which increases their vulnerability to social engineering, malware infections, and data leaks.

In addition to the technical and human challenges, policy gaps further weaken cybersecurity in online education. Some institutions lack clearly defined cybersecurity policies or fail to enforce existing guidelines effectively. There may be no incident response plan, no data encryption standards, or inconsistent protocols for account management and password hygiene. Even when policies are in place, compliance is often low due to limited monitoring and enforcement mechanisms. These systemic gaps hinder the development of a resilient security posture, making online education systems persistently vulnerable to attack.

Cybersecurity Frameworks and Best Practices

In the modern digital environment, the implementation of cybersecurity frameworks and best practices has become crucial for protecting information systems, particularly in sensitive sectors such as education. Cybersecurity frameworks provide structured guidelines and standards that organizations can adopt to safeguard digital assets, manage risks, and respond to cyber incidents effectively. These frameworks are especially important for institutions operating online learning platforms, where the confidentiality, integrity, and availability of data must be continuously ensured. According to Tabrizi and Liao (2021), the use of well-established cybersecurity frameworks enables institutions to adopt a proactive rather than reactive posture toward cyber threats.

One of the most widely recognized cybersecurity frameworks is the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This framework comprises five key functions—Identify, Protect, Detect, Respond, and Recover—that guide organizations in building resilient security infrastructures. In educational settings, applying the NIST framework helps administrators and IT personnel understand the types of assets that need protection, develop access controls, implement monitoring systems, and prepare recovery strategies in case of breaches (NIST, 2020). The flexibility of the NIST framework allows it to be adapted to a variety of institutional sizes and technological capacities, making it a suitable choice for universities, including those in developing regions.

In addition to NIST, the International Organization for Standardization's ISO/IEC 27001 standard is another globally accepted cybersecurity framework that outlines best practices for information security management systems (ISMS). It emphasizes the importance of continuous risk assessment, policy formulation, and staff training in maintaining cybersecurity resilience. Educational institutions that adopt ISO/IEC 27001 benefit from a culture of information security governance and are better positioned to maintain trust among stakeholders (Peltier, 2022). Though ISO/IEC certification may require considerable investment, its structured approach is invaluable in building long-term security maturity, especially as cyber threats grow more sophisticated.

Best practices in cybersecurity extend beyond adherence to frameworks—they also include day-to-day strategies that reduce risk. These practices involve a mix of technological solutions, administrative procedures, and user awareness initiatives. For instance, regular software updates and patch management help prevent the exploitation of known vulnerabilities. Institutions should also enforce multi-factor authentication (MFA), implement strong password policies, and encrypt sensitive data both at rest and in transit (Alghamdi *et al.,* 2020). Routine penetration testing and vulnerability assessments are essential for identifying system weaknesses before malicious actors can exploit them.

Human factors remain one of the weakest links in cybersecurity. Many breaches occur due to social engineering, phishing, or inadvertent errors by staff and students. Therefore, ongoing cybersecurity awareness training is a critical best practice that should be incorporated into institutional policy. Training should be tailored to different user groups—administrators, lecturers, IT personnel, and students—so that each group understands the risks relevant to their roles and responsibilities. According to Gkioulos *et al*. (2020), institutions that invest in cultivating cybersecurity-conscious cultures experience fewer breaches and recover more quickly when attacks do occur.

For developing nations, the adoption of cybersecurity frameworks and best practices must be supported by government policies and cross-institutional collaboration. In Nigeria, for example, the National Cybersecurity Policy and Strategy outlines the country's goals for securing critical digital infrastructure, including educational systems. However, implementation remains inconsistent across institutions due to lack of funding, inadequate expertise, and limited access to security technologies (Ogundokun & Salman, 2021). Consequently, partnerships with international cybersecurity organizations, public-private collaboration, and investment in local capacity building are necessary to support the effective rollout of best practices in educational institutions.

User Awareness and Cyber Hygiene in Academic Institutions

In today’s digitized academic environment, user awareness and cyber hygiene have become indispensable components of institutional cybersecurity. As more learning, teaching, and administrative tasks transition

online, academic institutions face growing risks related to poor digital practices by users—including students, faculty, and administrative staff. User awareness refers to the extent to which individuals understand the cybersecurity risks associated with their online behavior, while cyber hygiene encompasses the routine practices and precautions users take to maintain the security and integrity of their digital environment. Without adequate awareness and adherence to cyber hygiene protocols, even the most robust cybersecurity infrastructure can be undermined by human error or negligence (Tiwari & Joshi, 2020).

One of the primary challenges in academic institutions is the diversity of users with varying levels of technical knowledge. Students, particularly at the undergraduate level, often lack a basic understanding of cybersecurity principles and may engage in risky behaviors such as using weak passwords, ignoring software updates, or clicking suspicious links. Similarly, some faculty members and non-technical administrative staff may not be well-versed in secure data handling practices. According to Alotaibi (2020), many cyber incidents in universities stem not from sophisticated hacking attempts but from simple mistakes like sharing passwords, mishandling sensitive information, or falling for phishing schemes. These errors are often avoidable through regular training and a stronger culture of cybersecurity awareness.

User training and education are essential to foster good cyber hygiene in academic settings. Institutions that provide regular, tailored training programs for their users tend to experience fewer cyber incidents. These programs should cover topics such as password security, phishing detection, safe browsing habits, data protection policies, and secure use of institutional platforms. Cybersecurity awareness campaigns can also be integrated into orientation sessions for new students and staff, ensuring that cybersecurity becomes part of the academic culture from the onset. As Olalekan *et al*. (2022) observed, periodic cybersecurity workshops and digital awareness seminars have been effective in reducing user-based vulnerabilities in Nigerian universities.

Another vital aspect of cyber hygiene is the implementation of institutional policies that guide user behavior. Policies related to password management, acceptable use of university networks, and reporting of suspicious activities help establish expectations and accountability. However, these policies are only effective when users understand and adhere to them. Many institutions struggle with low policy compliance due to lack of clarity, communication gaps, or a perceived disconnect between IT departments and academic users. To bridge this gap, institutions must create user-friendly guidelines and ensure that cybersecurity protocols are accessible, understandable, and regularly updated (Khan *et al.,* 2021).

Technological tools also play a role in supporting good cyber hygiene. For instance, enforcing multi-factor authentication (MFA), automatic logout features, and periodic password change requirements can encourage users to adopt secure practices. Additionally, system reminders for software updates and anti-malware scans help users maintain clean and secure digital environments. However, over-reliance on technology without user engagement can create a false sense of security. As highlighted by Abubakar and Musa (2021), cybersecurity in academia is most effective when human behavior and technology are aligned through consistent communication and collaboration.

In developing countries like Nigeria, the need for user awareness and cyber hygiene is particularly acute due to limited resources and infrastructural challenges. Many students and staff access institutional platforms using personal devices, often shared with others and lacking updated security software. This further complicates the cybersecurity landscape. Institutions must therefore adopt a multi-pronged approach that combines awareness programs, clear policies, accessible technologies, and continuous user engagement. Capacity-building efforts should be supported by national policies that promote digital literacy and prioritize cybersecurity education at all levels of academia.

Challenges to Implementing Cybersecurity Measures in Developing Countries

The implementation of cybersecurity measures in developing countries is fraught with a myriad of complex challenges that extend beyond technological constraints. These challenges are deeply rooted in infrastructural limitations, policy inadequacies, insufficient expertise, economic barriers, and a general lack of cybersecurity awareness. As the digital transformation accelerates across global sectors—including education, healthcare, finance, and governance—the vulnerability of developing nations to cyberattacks has increased significantly. While the need for cybersecurity is widely acknowledged, these nations often lack the critical foundation needed to design, implement, and sustain effective cybersecurity strategies (Ogu *et al.,* 2021).

One of the most pressing challenges is the limited availability of infrastructure and financial resources. Robust cybersecurity requires substantial investment in hardware, software, personnel, and training. However, many developing countries are still struggling to provide reliable electricity, internet connectivity, and basic digital infrastructure. This financial constraint forces governments and institutions to prioritize other urgent socio-economic needs over cybersecurity. As a result, cybersecurity efforts are often underfunded, reactive, and fragmented. According to Chigada and Madzinga (2020), many African countries allocate less than 1% of their national budgets to

cybersecurity development, which is grossly inadequate in the face of growing threats.

Equally important is the shortage of skilled cybersecurity professionals. Developing countries face a significant talent gap in the cybersecurity field due to weak educational pipelines and brain drain, where trained experts migrate to developed countries for better job prospects. This shortage leaves government agencies, educational institutions, and private organizations unable to recruit or retain qualified personnel to design, monitor, and maintain secure systems. In the absence of in-house expertise, many institutions rely on outdated security configurations or off-the-shelf solutions that are not tailored to their specific needs. As reported by Kwet (2019), the lack of localized cybersecurity solutions exacerbates vulnerability, as institutions often depend on foreign software and platforms that may not comply with local regulatory and security contexts.

Policy and legal frameworks also present significant hurdles. In many developing countries, cybersecurity legislation is either outdated, poorly enforced, or nonexistent. The absence of comprehensive laws to address cybercrime, data privacy, and digital governance makes it difficult to hold perpetrators accountable and discourages victims from reporting incidents. Even when laws exist, enforcement mechanisms are weak due to inadequate policing resources, lack of digital forensic capabilities, and judicial inexperience with cyber-related cases. Aluko and Adedoyin (2022) note that in Nigeria, despite the enactment of the Cybercrimes Act in 2015, implementation remains inconsistent, and public institutions frequently operate without clear cybersecurity policies or response protocols.

Another significant challenge is the low level of cybersecurity awareness among end-users. Many citizens, including students, civil servants, and small business owners, are unfamiliar with basic cybersecurity practices such as using strong passwords, identifying phishing attempts, or securing personal devices. This lack of awareness results in behaviors that expose systems to threats and make institutional cybersecurity efforts less effective. According to Akinyemi and Kure (2020), cybersecurity is often perceived as a purely technical issue in developing countries, with little emphasis placed on user education or community involvement in maintaining digital security.

In addition, geopolitical and economic dependencies present subtle challenges. Many developing countries rely heavily on foreign technology providers for their digital infrastructure, which can pose national security risks. These dependencies make it difficult for governments to assert control over their cyberspace and often result in weak negotiation power when dealing with multinational technology companies. Moreover, there are concerns about surveillance, data sovereignty, and the ethical implications of adopting foreign technologies without full transparency. These concerns underscore the importance of developing indigenous cybersecurity capacities, which are currently lacking in most developing nations (Mothibi & Mncube, 2021).

Lastly, corruption and lack of political will often hinder cybersecurity advancement. In some cases, cybercrime is not treated as a national security issue, and the absence of political commitment means that cybersecurity programs do not receive sustained support. Procurement processes for cybersecurity tools may also be riddled with inefficiencies or mismanagement, leading to the acquisition of inappropriate technologies or misallocation of resources. As highlighted by Abdullahi *et al*. (2021), institutional corruption and weak governance structures are major roadblocks in implementing a coordinated and effective national cybersecurity strategy.

Theoretical Framework

Protection Motivation Theory (PMT)

The Protection Motivation Theory (PMT) was originally proposed by Rogers (1975) in his work on fear appeals and behavior change. Initially, it was used to explain how individuals are motivated to protect themselves from health threats, but over the years, its application has expanded to a variety of fields, including cybersecurity, where it is used to understand the behaviors, individuals take to protect their digital environments. Rogers formulated PMT to explain how fear, combined with certain cognitive processes, can motivate individuals to engage in protective behaviors. Specifically, he sought to understand how threats, when perceived as severe, lead individuals to adopt protective measures, especially when they feel that they can take steps to mitigate or avoid those threats. This theory was based on the idea that the perception of risk and the belief in one's ability to counteract the threat are key drivers in motivating action to reduce harm (Rogers, 1975).

The core premise of PMT is that individuals assess the severity and probability of a threat and their ability to cope with that threat, which influences their behavior in terms of adopting protective measures. PMT suggests that individuals are more likely to engage in preventive actions if they perceive a threat as serious and within their ability to control or mitigate. In the context of cybersecurity, this would mean that individuals are more likely to engage in safe online practices if they believe in the severity of cyber threats and their ability to protect their personal information (Baker & Jones, 2021).

The Protection Motivation Theory includes the following key principles:

i. Perceived Severity: The belief that a threat is serious or dangerous.

ii. Perceived Vulnerability: The belief that one is at risk or vulnerable to the threat.
iii. Response Efficacy: The belief that the recommended protective behaviors will effectively reduce the threat.
iv. Self-Efficacy: The belief in one's ability to perform the recommended protective behaviors.
v. Fear: The emotional response to the perceived threat, which can influence the motivation to act.
vi. Response Costs: The perceived costs or barriers to performing the protective behaviors (e.g., time, effort, money).

PMT is highly relevant in today's society as it addresses how individuals react to perceived threats, particularly in the realm of cybersecurity. In an era of digital transformation, where cyber threats such as identity theft, hacking, and data breaches are commonplace, PMT provides a framework for understanding why people take (or fail to take) protective actions. It underscores the importance of not only educating users about the risks but also building their confidence in the ability to act against those threats. For example, if individuals believe they are vulnerable to a cyber-attack but also believe that using strong passwords or activating multi-factor authentication will help mitigate that threat, they are more likely to adopt these practices.

The current study, which examines the effectiveness of cybersecurity measures in safeguarding online educational resources at the University of Port Harcourt, is directly applicable to the Protection Motivation Theory. The theory can help explain how faculty, students, and administrative staff perceive the cybersecurity threats to the university's online learning platform. By assessing their perceived severity of cyber threats, their perceived vulnerability (e.g., risk of data breaches or unauthorized access), and their confidence in being able to adopt the recommended protective measures, the study can gain insights into user behavior and attitudes towards cybersecurity in higher education. PMT can thus help evaluate the motivations behind users' cybersecurity practices and guide the design of interventions that are aimed at increasing security measures through tailored fear appeals and educational programmers.

Empirical Reviews

Ogunleye and Olanrewaju (2020) conducted a study to assess the effectiveness of cybersecurity awareness programs within Nigerian universities, highlighting the critical role of awareness in mitigating cyber risks. The authors examined how cybersecurity training programs influenced the knowledge and attitudes of students and faculty members toward digital security. Using a mixed-methods approach, the researchers surveyed 250 students and faculty from three universities, including interviews and a structured questionnaire. The study found that although awareness programs improved knowledge and behaviors regarding safe online practices, the implementation was hindered by irregular training sessions and inadequate resources. Furthermore, the study suggested that the lack of enforcement and follow-up initiatives resulted in a decline in awareness over time. The results emphasize the need for more consistent and structured awareness programs to ensure lasting behavioral changes, which is critical for safeguarding online learning environments. This finding resonates with the current study, which seeks to understand the effectiveness of cybersecurity measures in educational institutions, particularly in the context of open and distance learning.

Ahmed and Khalid (2021) explored cybersecurity challenges faced by South Asian universities, particularly in the context of online education. The study examined how universities were coping with cybersecurity threats amid the rapid shift to online learning during the COVID-19 pandemic. Through qualitative interviews with 15 IT administrators and faculty members from six universities, the study identified several recurring cybersecurity issues, including weak password practices, inadequate data protection measures, and insufficient training for staff and students. Additionally, the authors found that while some universities had implemented basic cybersecurity protocols, there was a lack of comprehensive strategies for securing online learning platforms. The study concluded that the institutions' cybersecurity frameworks were reactive rather than proactive and that there was a need for more robust policies and ongoing user education. The findings align closely with the current study's focus on evaluating the adequacy and effectiveness of existing cybersecurity measures within the University of Port Harcourt's Open and Distance Learning system.

Gibson and Sinclair (2022) analyzed the gap between the formulation and implementation of cybersecurity policies in higher education institutions. Their study, which involved a survey of 120 academic and administrative staff across 10 universities in North America, revealed significant discrepancies between policy creation and actual enforcement. The researchers highlighted that while most universities had cybersecurity policies in place, a majority of the participants reported inadequate implementation, citing lack of resources, insufficient training, and low compliance among staff and students. The authors further noted that universities with clearer, more accessible policies and continuous staff training experienced fewer cyber incidents compared to those with vague or outdated policies. This study provides valuable insights into the broader challenges universities face in translating cybersecurity policies into practical, everyday protections for digital education systems. For the current study, this research underscores the

importance of not only formulating strong cybersecurity policies but also ensuring their effective implementation to safeguard online educational resources.

Williams and Park (2020) examined the cybersecurity risks and strategies adopted by educational institutions in developing countries, focusing on online learning platforms. The study, which surveyed 15 universities in sub-Saharan Africa, revealed that many institutions were unprepared for the surge in online education brought about by the COVID-19 pandemic. The researchers found that the majority of institutions lacked proper cybersecurity infrastructure and had weak incident response plans. Additionally, the study identified that faculty and students often bypassed security protocols due to lack of awareness and convenience factors, such as using unsecured networks or simple passwords. The study also explored various strategies, such as strengthening encryption, adopting multi-factor authentication, and providing regular cybersecurity training. The authors emphasized that universities in developing countries need to implement more rigorous and context-specific cybersecurity measures to effectively secure online learning environments. The findings from this study are particularly relevant to the current study as they highlight the cybersecurity risks faced by institutions in developing countries, providing a broader context for evaluating the University of Port Harcourt's cybersecurity measures.

METHODOLOGY

This study will adopt a quantitative research design, utilizing descriptive statistics to evaluate the effectiveness of cybersecurity measures in safeguarding online educational resources at the University of Port Harcourt's Open and Distance Learning (ODL) system. A structured questionnaire will be administered to a stratified random sample of 50 students, faculty, and administrative staff involved in the ODL system. The questionnaire will gather data on participants' awareness of existing cybersecurity measures, their perceived vulnerabilities, and their self-reported practices regarding cybersecurity. The data collected will be analyzed using descriptive statistics, specifically calculating the mean to determine the overall level of awareness, effectiveness, and engagement with cybersecurity practices within the ODL system. This approach will provide quantitative insights into the current state of cybersecurity within the university's online learning platform. Ethical considerations, such as informed consent and confidentiality, will be adhered to throughout the study.

RESULTS

Objective 1: To evaluate the effectiveness of existing cybersecurity measures implemented within the University of Port Harcourt's Open and Distance Learning (ODL) system in protecting online educational resources.

Table 1: Evaluating the Effectiveness of Existing Cybersecurity Measures

S/N	Statement	SA	A	N	D	SD	$\bar{x}$	Remark
1	The ODL platform has adequate firewall protection in place.	10	16	10	9	5	3.34	Neutral
2	Antivirus and anti-malware software are regularly updated.	12	15	11	8	4	3.46	Agree
3	User login systems on the ODL platform are secure and reliable.	12	18	7	7	6	3.46	Agree
4	Data encryption is used to protect sensitive educational resources.	12	15	10	9	4	3.44	Agree
5	There are clear procedures for reporting cybersecurity issues.	13	15	9	8	5	3.46	Agree
6	Security updates and patches are applied promptly.	14	15	8	7	6	3.48	Agree
7	Measures in place effectively reduce the risk of data breaches.	13	15	9	8	5	3.46	Agree

The analysis in Table 1, which evaluates the effectiveness of existing cybersecurity measures within the University of Port Harcourt's Open and Distance Learning (ODL) system, reveals a general perception of inadequacy among respondents. Across the seven statement items, the mean scores largely hover around 3.34 to 3.48 on a 5-point Likert scale, with most items receiving a "Agree" and just one item receiving a "Neutral" remark. This suggests that users are strongly convinced of the robustness of the existing cybersecurity infrastructure. Overall, this interpretation indicates that while some baseline cybersecurity measures may exist, their effectiveness in practice is not questionable and possibly determined by implementation process or user confidence.

Objective 2: To identify specific vulnerabilities and challenges affecting the cybersecurity infrastructure of the University's ODL platform, including user awareness, policy implementation, and technical controls.

Table 2: Identifying Specific Vulnerabilities and Challenges

S/N	Statement	SA	A	N	D	SD	$\bar{x}$	Remark
1	ODL users lack sufficient cybersecurity training.	14	18	9	6	3	3.68	Agree
2	Policies are poorly communicated to users.	16	16	8	7	3	3.70	Agree
3	There is a shortage of skilled IT personnel.	15	19	8	5	3	3.76	Agree
4	Students and staff often use weak passwords.	15	17	8	7	3	3.68	Agree

S/N	Statement	SA	A	N	D	SD	$\bar{x}$	Remark
5	There is inadequate funding for cybersecurity improvements.	15	15	7	8	5	3.54	Agree
6	Users access the ODL platform through unsecured networks.	16	16	8	7	3	3.70	Agree
7	Cybersecurity audits are not conducted regularly.	15	16	8	7	4	3.62	Agree

Table 2 focuses on identifying specific vulnerabilities and challenges to the cybersecurity infrastructure of the ODL system. The results present a more concerning picture, as the mean scores for most statement items fall between 3.54 and 3.76, with predominant "Agree" remarks. These scores signify that users perceive the existence of multiple critical challenges affecting cybersecurity performance. Notably, there is a shared belief that there is insufficient cybersecurity training, poor communication of security policies, and a shortage of skilled IT personnel. These issues are compounded by technical challenges such as the frequent use of weak passwords, unsecured network access, and irregular cybersecurity audits. The acknowledgment of funding inadequacies further highlights structural limitations that could be restricting the institution's capacity to secure its digital learning environment effectively. Collectively, these findings point to systemic vulnerabilities that could be exploited if not addressed urgently. The perceived challenges span human, administrative, and infrastructural dimensions, underscoring the need for a comprehensive and strategic response.

Objective 3: To propose strategic improvements and best practices for enhancing the cybersecurity framework of the University of Port Harcourt's ODL system based on empirical findings.

Table 3: Probable Strategies for Improvement and Best Practices

S/N	Statement	SA	A	N	D	SD	$\bar{x}$	Remark
1	Regular cybersecurity awareness training should be mandatory for all ODL users.	20	23	3	2	2	4.14	Strongly Agreed
2	The ODL system should implement multi-factor authentication for all user logins.	18	22	5	3	2	4.02	Agreed
3	Continuous vulnerability assessments and audits should be conducted periodically.	17	20	7	3	3	3.90	Agreed
4	Cybersecurity policy enforcement should be strengthened with clear sanctions.	15	22	7	3	3	3.86	Agreed
5	There is a need to upgrade the technical infrastructure of the ODL platform.	17	18	8	4	3	3.84	Agreed
6	Appointing a dedicated cybersecurity officer for the ODL unit is essential.	13	20	10	3	4	3.70	Agreed
7	Security best practices should be integrated into the ODL curriculum.	12	22	10	3	3	3.74	Agreed

Table 3 focuses on evaluating proposed strategic improvements and best practices for enhancing the cybersecurity framework of the University of Port Harcourt's Open and Distance Learning (ODL) system. The results reveal generally positive stakeholder perceptions, with mean scores ranging from 3.80 to 4.40 and predominant "Agreed" and "Strongly Agreed" remarks. These scores suggest a strong consensus on the necessity of implementing targeted cybersecurity enhancements. Notably, there is overwhelming support for mandatory cybersecurity awareness training and the adoption of multi-factor authentication, indicating a recognition of the need to strengthen user-level defenses. Participants also expressed agreement on the importance of conducting periodic vulnerability assessments, enforcing cybersecurity policies with defined sanctions, and upgrading technical infrastructure to better safeguard online educational resources. Additionally, there is a favorable perception of appointing a dedicated cybersecurity officer and incorporating security best practices into the academic curriculum. Collectively, these findings reflect a shared understanding that a proactive, well-resourced, and education-centered cybersecurity approach is essential for the long-term resilience and credibility of the ODL system. The responses highlight actionable pathways for institutional improvement across technical, administrative, and pedagogical dimensions.

DISCUSSION OF FINDINGS

The findings from this study provide a nuanced view of the cybersecurity landscape within the University of Port Harcourt's Open and Distance Learning (ODL) system, especially when viewed through the lens of the two stated objectives. While there appears to be a level of confidence in the effectiveness of some of the cybersecurity measures in place, there is a parallel recognition of pressing vulnerabilities and systemic challenges that threaten the reliability and security of the online education infrastructure.

Evaluation of Existing Cybersecurity Measures

The responses gathered in relation to the first objective indicate that users are, to a considerable extent,

convinced of the robustness of the current cybersecurity infrastructure implemented within the ODL platform. The mean scores, which generally trended toward neutrality or mild agreement, suggest that users acknowledge the presence of baseline technical defenses such as firewalls, antivirus systems, and encryption protocols. This perceived adequacy reflects positively on the efforts of the university's ICT unit and aligns with the fundamental premise of cybersecurity practice, which is to establish multiple layers of defense to safeguard information assets. These findings resonate with the assertions of Alshaikh (2020), who emphasized that the strength of a cybersecurity system is not merely in its technological tools but also in how these tools are integrated and maintained to ensure holistic protection. According to Alshaikh, an organization's cybersecurity posture is significantly shaped by its ability to implement consistent and reliable technical controls, and the results from this study suggest that such mechanisms may be partially in place at the University of Port Harcourt. However, the fact that most responses still leaned towards neutrality indicates that while there may be infrastructure, full user confidence in its reliability is yet to be firmly established. This reflects a common trend in higher education institutions where cybersecurity is implemented, but users are either unaware of its breadth or unsure of its effectiveness due to limited transparency or engagement.

Identification of Specific Vulnerabilities and Challenges

Contrastingly, findings from the second objective reveal a more critical insight — the users' perception of numerous vulnerabilities and systemic challenges that impede the full realization of cybersecurity effectiveness. Participants consistently agreed that there are gaps in user training, weak password practices, under-communication of policies, lack of skilled IT personnel, and insufficient audit mechanisms. These perceptions strongly suggest that even though infrastructure may exist, it is undermined by operational and human factors, which are equally vital components of any robust cybersecurity strategy. This aligns closely with the observations of Azevedo and Marques (2021), who noted that in developing contexts, especially within higher education, cybersecurity efforts are often frustrated not by a lack of awareness of threats, but by an inability to implement sustainable countermeasures due to budgetary constraints, weak institutional frameworks, and low user engagement. Their study emphasized the need for higher education institutions to integrate cybersecurity as a strategic priority that cuts across technical, administrative, and behavioral domains. The findings from this study support this perspective, illustrating that while the University of Port Harcourt may have made initial strides in deploying cybersecurity technology, the broader ecosystem — which includes training, funding, monitoring, and responsive policy — remains underdeveloped.

Probable Strategies for Improvement and Best Practices

The findings from the third objective present a constructive perspective on enhancing cybersecurity in the University of Port Harcourt's ODL system through strategic improvements and best practices. Participants showed a high level of agreement on the importance of measures such as regular cybersecurity awareness training, the implementation of multi-factor authentication, periodic vulnerability assessments, and enforcement of cybersecurity policies with defined sanctions. These findings demonstrate a strong stakeholder consensus that cybersecurity must be approached as an integrated system involving not only technology but also people, processes, and institutional policies. This is consistent with the work of Ngwa (2020), who emphasized in his study on cybersecurity in African higher education institutions that the effectiveness of digital security frameworks largely depends on user participation, policy alignment, and continuous training. Ngwa observed that while many institutions invest in technical infrastructure, they often neglect the human and administrative dimensions of cybersecurity, leading to persistent vulnerabilities. His study called for a holistic cybersecurity approach that incorporates governance, user behavior, and curriculum-based interventions—a view clearly echoed by the responses in this study. Participants in the current research also recognized the need to upgrade technical infrastructure, appoint dedicated cybersecurity personnel, and integrate cybersecurity awareness into the learning curriculum. These findings align with Ngwa's recommendation for institutional capacity-building through dedicated cybersecurity leadership and education-driven awareness strategies. In essence, this study supports and extends existing literature by affirming that meaningful cybersecurity enhancement in ODL environments requires a multi-faceted approach—one that balances technical upgrades with policy reform, user education, and consistent monitoring.

CONCLUSION

This study set out to evaluate the effectiveness of cybersecurity measures implemented within the University of Port Harcourt's Open and Distance Learning (ODL) system, and to identify specific vulnerabilities and challenges affecting its cybersecurity infrastructure. The findings reveal a dual reality: while there is a moderate level of user confidence in the existing technological safeguards such as firewalls, antivirus tools, and data encryption mechanisms, there are nonetheless significant and persistent concerns regarding the broader cybersecurity framework, especially in areas related to user behavior, institutional policy, technical expertise, and infrastructural support. The study's analysis shows that many users believe the foundational security systems are in place, but their overall effectiveness is diluted by weak implementation practices, inadequate training, poor policy communication, and insufficient audit and funding

mechanisms. These gaps highlight that cybersecurity cannot be sustained by technical tools alone—it must be embedded within the institutional culture, supported by strategic planning, regular training, continuous policy enforcement, and adequate resource allocation.

Drawing on empirical insights and supported by reviewed literature, it becomes evident that universities, especially in developing contexts like Nigeria, must adopt a more holistic, multi-layered approach to cybersecurity. Institutions must ensure that both technological and human factors are addressed cohesively to effectively safeguard digital learning environments. For the University of Port Harcourt, this means investing not only in infrastructure but also in cybersecurity awareness campaigns, routine system audits, and the continuous upskilling of IT personnel. In conclusion, the effectiveness of cybersecurity within the ODL platform at the University of Port Harcourt is currently compromised by overlooked human and administrative vulnerabilities. Addressing these concerns proactively is essential not only to protect online educational resources but also to sustain the credibility, accessibility, and security of digital learning in the evolving educational landscape.

RECOMMENDATIONS

Based on the findings, discussions and conclusion made, the following recommendations were made:

1. The ICT unit should establish a comprehensive and continuous cybersecurity audit and monitoring protocol.
2. The coordinator should integrate mandatory cybersecurity awareness and training sessions into student and staff orientation.
3. A dedicated budget should be allocated annually for cybersecurity upgrades, policy enforcement, and capacity building.
4. Clear, accessible, and regularly updated cybersecurity policies should be drafted and widely disseminated to all ODL users.
5. Targeted recruitment and continuous professional development of cybersecurity professionals should be prioritized.

REFERENCES

- Abdullahi, M. B., Musa, A. A. & Sani, S. I. (2021). Challenges of cybersecurity development in Nigeria: Institutional frameworks and policy gaps. *Journal of African Cyber Policy and Governance, 4*(1), 66–80.
- Abubakar, A. M. & Musa, I. H. (2021). Human factors in cybersecurity: A study of Nigerian university systems. *African Journal of Information Systems, 13*(2), 157–175.
- Adebayo, F. & Kehinde, F. (2022). Cybersecurity preparedness in Nigerian universities: Challenges and strategies. *Journal of Cybersecurity Education, Research and Practice, 2022*(1), Article 3.
- Adebesin, F. & Shange, M. (2021). A critical review of cybersecurity readiness in Nigerian higher education institutions. *African Journal of Information and Communication, 28*(1), 42–59.
- Adedoyin, O. B. & Soykan, E. (2020). COVID-19 pandemic and online learning: The challenges and opportunities. *Interactive Learning Environments*, 1–13.
- Ahmed, H. M. & Khalid, S. (2021). Cybersecurity challenges in online education systems: A study of South Asian universities. *International Journal of Cybersecurity in Education, 5*(3), 175–190.
- Akinyemi, I. O. & Kure, H. I. (2020). The role of user awareness in enhancing cybersecurity in Nigeria's digital economy. *African Journal of Information Systems, 12*(2), 101–117.
- Alasmary, W., Alhaidari, F. & Alghamdi, M. (2022). Cybersecurity awareness and practices among university students and staff: A case study. *International Journal of Advanced Computer Science and Applications (IJACSA), 13*(4), 456–462.
- Al-Fraihat, D., Joy, M., Sinclair, J. & Alrahmi, W. (2020). Evaluating E-learning systems success: An empirical study. *Computers in Human Behavior, 102*, 67–86.
- Alghamdi, A., Alenazi, M. & Alrashed, H. (2020). Cybersecurity practices in higher education: A comprehensive review. *International Journal of Advanced Computer Science and Applications (IJACSA), 11*(6), 77–85.
- Alharthi, R., Krotov, V. & Bowman, M. (2020). Addressing cybersecurity challenges of online education. *Journal of Theoretical and Applied Electronic Commerce Research, 15*(1), 1–13.
- Alotaibi, M. B. (2020). Cybersecurity awareness among university students: A case study. *International Journal of Computer Applications, 176*(28), 25–30.
- Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*, 102003.
- Aluko, T. & Adedoyin, O. (2022). Cybersecurity laws and their implementation challenges in Nigeria. *International Journal of Cyber Law and Policy, 6*(2), 34–49.
- Baker, M. A. & Jones, R. M. (2021). Protection motivation theory in cybersecurity: Implications for user behavior and intervention strategies. *Journal of Cybersecurity Awareness, 12*(3), 210–225.
- Cheng, X. & Jin, Y. (2021). Cybersecurity challenges in remote education: Lessons from the COVID-19 pandemic. *Education and Information Technologies, 26*, 7441–7456.
- Chigada, J. & Madzinga, R. (2020). Cybersecurity awareness in developing countries: A comparative study of African states. *Information and Computer Security, 28*(3), 291–308.

- Dhawan, S. (2020). Online learning: A panacea in the time of COVID-19 crisis. *Journal of Educational Technology Systems, 49*(1), 5–22.
- Fikri, M. R. & Setiawan, B. (2021). Analysis of security vulnerabilities in online learning platforms. *International Journal of Cyber Security and Digital Forensics, 10*(3), 229–238.
- Gibson, A. R. & Sinclair, E. (2022). Cybersecurity policies in higher education: An analysis of the gap between policy formulation and implementation. *Journal of Higher Education Policy and Management, 44*(1), 45–61.
- Gkioulos, V., Kostopoulos, G., Eklund, P. & Katsikas, S. (2020). Security awareness in academia: Building a cybersecurity culture. *Education and Information Technologies, 25*(4), 2949–2972.
- Hewitt, R. J., Turner, D. & Owens, R. (2021). Cyber risk management in higher education: A practical framework. *Information & Computer Security, 29*(1), 81–97.
- Johnson, C., Wagner, J. & Cooper, J. (2021). The impact of ransomware attacks on higher education institutions. *Information Security Journal: A Global Perspective, 30*(2), 87–97.
- Khan, R., Alshareef, R. & Raza, A. (2021). Enhancing cybersecurity awareness in academic institutions through policy-driven training programs. *Journal of Information Security Research, 12*(1), 34–45.
- Kirkwood, A. & Price, L. (2021). Technology-enhanced learning and teaching in higher education: What is 'enhanced' and how do we know? *A Journal of Learning and Technology, 46*(2), 176–195.
- Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the Global South. *Race & Class, 60*(4), 3–26.
- Mothibi, G. & Mncube, S. (2021). Technology dependence and cybersecurity threats in sub-Saharan Africa: An institutional analysis. *Journal of Digital Security Studies, 3*(1), 45–62.
- Mseleku, Z. (2020). A literature review of E-learning and E-teaching in the era of COVID-19 pandemic. *South African Journal of Higher Education, 34*(5), 114–132.
- National Institute of Standards and Technology. (2020). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- Ogu, J. O., Nwakanma, I. C. & Okoli, I. E. (2021). Strengthening cybersecurity in Africa: Challenges and policy perspectives. *Journal of African Technology Studies, 15*(1), 81–98.
- Ogundokun, R. O. & Salman, Y. B. (2021). Assessment of cybersecurity strategies in Nigerian universities: Policy implications. *African Journal of Information and Communication, 28*, 61–77.
- Ogunleye, I. & Olanrewaju, S. O. (2020). Assessing the effectiveness of cybersecurity awareness programs in Nigerian higher education institutions. *African Journal of Educational Technology, 6*(2), 99–112.
- Olalekan, O. J., Omotunde, A. J. & Ezeanya, P. I. (2022). Evaluating the impact of cybersecurity training in Nigerian tertiary institutions. *Journal of Educational Technology and Society, 25*(2), 101–113.
- Osuagwu, O. E. & Chukwudebe, G. A. (2022). Evaluating cybersecurity readiness in Nigerian universities: A case study approach. *Nigerian Journal of Technology (NIJOTECH), 41*(4), 702–710.
- Patil, M. B. & Patil, P. K. (2020). Cybersecurity threats in e-learning and remote learning systems: A study of security concerns in academic institutions. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 6*(3), 53–59.
- Peltier, T. R. (2022). *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management* (2nd ed.). Auerbach Publications.
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93–114.
- Salloum, S. A., Al-Emran, M. & Shaalan, K. (2021). The impact of COVID-19 on cybersecurity in online education: A stakeholder perspective. *Education and Information Technologies, 26*(4), 4181–4197.
- Susanto, H. & Almunawar, M. N. (2020). Cybersecurity in higher education: A systematic review. In: M. S. Obaidat *et al*. (Eds.), Proceedings of the 2020 *International Conference on Information and Communication Technology (ICICT)* (pp. 320–330). Springer.
- Tabrizi, B. & Liao, S. (2021). Building cyber resilience in education: Frameworks and implementation strategies. *Cybersecurity Trends, 8*(2), 104–119.
- Tiwari, A. & Joshi, A. (2020). Promoting cyber hygiene through awareness: Role of academic institutions. *International Journal of Information Security Science, 9*(3), 145–154.
- UNESCO. (2020). *Education in a post-COVID world: Nine ideas for public action*. https://unesdoc.unesco.org/ark:/48223/pf0000373717
- Williams, M. J. & Park, S. (2020). Cybersecurity risks and strategies for online educational platforms in developing countries. *Educational Technology & Society, 23*(4), 32–45.
- Zhang, W., Cheng, J. & Li, H. (2021). The effectiveness of online education in a pandemic: A study of student satisfaction and learning outcomes. *Education and Information Technologies, 26*, 3385–3403.